DUMPSBOSS.

# Certified Information Privacy Professional/Asia (CIPP/A)

## IAPP CIPP-A

## Version Demo

**Total Demo Questions: 12**

**Total Premium Questions: 128**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Introduction to Privacy | 9 |
| Topic 2, Asia-Pacific Privacy Laws and Regulations | 88 |
| Topic 3, Jurisdictional Laws and Regulations | 31 |
| Total | 128 |

QUESTION NO: 1

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.

**ANSWER: C**

**Explanation:**

“Adds a provision about wrongful loss or gain.” is correct because Section 72A of India’s Information Technology Act, 2000 makes the actor’s intent central to the offence. It applies where a person has obtained access to personal information while providing services under the terms of a lawful contract and, with the intent to cause, or knowing that disclosure is likely to cause, wrongful loss or wrongful gain, discloses that information without the concerned person’s consent. This wrongful-loss-or-gain element is an important distinguishing feature in the statutory wording of Section 72A. The provision addresses improper disclosure of personal information in a contractual service relationship and connects liability to the requisite harmful intent or knowledge. This helps distinguish the specific breach-of-contract disclosure offence under Section 72A from the broader confidentiality and privacy duty addressed elsewhere in the Act. The statutory text can be consulted in the official Information Technology Act, 2000; see Section 72A. India’s Ministry of Electronics and Information Technology also provides the Act among its cyber-law resources.

**QUESTION NO: 2**

SCENARIO â€“ 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.

**ANSWER: D**

**Explanation:**

**Up to five years imprisonment.** is correct. Part VIA of Hong Kong's Personal Data (Privacy) Ordinance establishes specific rules for providing personal data to another person for that person's use in direct marketing. Where personal data are provided in return for gain, the transferor must have taken the prescribed steps, including giving the data subject the required information and obtaining the required consent. The scenario expressly assumes Kelvin received a commission, which constitutes a transfer for gain, and that the recipient used Stephen's contact details for direct marketing. Kelvin's former employment does not shield him from personal criminal exposure for a knowing disclosure of the client information for his own gain. Under section 35J, contravention of the provisions governing provision of personal data for gain for direct-marketing use is an offence carrying, on conviction, a maximum fine of HK$1,000,000 and imprisonment for five years. The five-year maximum is therefore the applicable imprisonment penalty described in the available answers. The statutory direct-marketing provisions appear in Part VIA of the Personal Data (Privacy) Ordinance. The Hong Kong Privacy Commissioner also summarizes the consent and notification obligations for transfers of personal data used in direct marketing in its Guidance Note on Direct Marketing.

## QUESTION NO: 3

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.

**ANSWER: D**

**Explanation:**

**Unreasonable expense.** is the best answer because the APEC Privacy Framework recognizes that an organization's obligation to provide an individual access to personal information is qualified in limited circumstances. In particular, access need not be provided where the burden or expense of doing so would be disproportionate to the privacy risks faced by the individual in the particular case. This qualification reflects a practical, risk-based application of the Access and Correction principle: individuals should ordinarily be able to obtain and correct their personal information, but an organization is not expected to incur a disproportionate operational or financial burden for an access request where the privacy impact does not justify it.

The Framework also emphasizes that any limitation should remain narrow and should be applied consistently with the overall objective of protecting personal information. Organizations should therefore assess the specific request, the likely privacy consequences for the individual, and the actual burden or expense involved rather than treating access as categorically unavailable. The relevant language appears in the Access and Correction principle of the APEC Privacy Framework. See the APEC Privacy Framework (2015) and APEC's Electronic Commerce Steering Group resources.

## QUESTION NO: 4

Which of the following is a key obligation of a business operator handling pseudonymously processed information under Japan's APPI?

**A.** It must publish all pseudonymization algorithms used.

**B.** It must not use the information to contact the individual.

**C.** It must delete the information within 30 days.

**D.** It must obtain new consent before any internal use of the information.

**ANSWER: B**

**Explanation:**

**It must not use the information to contact the individual.** is correct. Pseudonymously processed information under Japan's APPI is information created through prescribed processing that makes it difficult to identify a specific individual unless other information is collated. It remains regulated information, but certain APPI obligations are adjusted to facilitate secure internal analysis and similar uses.

A key restriction is that a business operator handling pseudonymously processed information must not use that information to contact the individual concerned. It must also take security-control measures and is generally prohibited from providing the information to third parties, subject to limited statutory exceptions. Pseudonymization is therefore not equivalent to anonymization and does not permit unrestricted use or disclosure. See the Act on the Protection of Personal Information and the Personal Information Protection Commission's legal resources.

## QUESTION NO: 5

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.

**ANSWER: B**

**Explanation:**

Companies researching the viability of business mergers is correct because Hong Kong's Personal Data (Privacy) Ordinance includes a specific exemption for personal-data transfers made for a due-diligence exercise connected with a proposed business transaction. The provision is intended to let parties assess a contemplated transaction—such as a merger, acquisition, sale of business or assets, restructuring, or similar change in ownership or control—where access to relevant personal data may be necessary to evaluate the transaction's viability, value, risks, or operational implications.

The exemption is limited rather than a general permission to disclose data during commercial discussions. It applies where the disclosure is genuinely for due diligence relating to a proposed transaction, and the recipient must not use the data for a purpose other than that due-diligence exercise. The statutory framework also preserves the Ordinance's broader privacy protections and does not remove the need for appropriate safeguards, confidentiality controls, and data minimisation. This reflects the practical need to allow legitimate corporate transaction reviews without treating every necessary disclosure as incompatible with the data-use principle. The relevant statutory provision is section 63B of the PDPO; see the Personal Data (Privacy) Ordinance on Hong Kong e-Legislation and the PCPD's guidance on cross-border data transfers.

## QUESTION NO: 6

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.

**ANSWER: B**

**Explanation:**

Health information is considered sensitive personal information in almost all privacy-law frameworks because it reveals intimate details about an individual's physical or mental condition, medical treatment, disability, genetic predispositions, and health-care needs. Misuse or unauthorized disclosure can lead to serious harms, including stigma, discrimination, loss of employment opportunities, financial harm, or unwanted exposure of highly private circumstances. Consequently, privacy regimes commonly impose heightened requirements for collecting, using, disclosing, securing, and retaining health data. For example, the GDPR treats data concerning health as a special category of personal data and generally prohibits its processing unless a specified condition applies, such as explicit consent, medical care, public-health purposes, or a substantial public-interest basis. Across Asia, while statutory terminology and specific obligations differ by jurisdiction, health information is consistently recognized as requiring enhanced protection. This broad international consensus makes health information the best single answer to a question asking which category is sensitive in almost all countries with privacy laws. See the GDPR's definition and protections for health data in Articles 4 and 9 of Regulation (EU) 2016/679, and the IAPP overview of sensitive personal information.

## QUESTION NO: 7

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.** The Safe Harbor Framework.

**D.** Binding Corporate Rules (BCR).

**ANSWER: C**

**Explanation:**

The Safe Harbor Framework could not be used as a legitimate GDPR transfer mechanism because it was invalidated by the Court of Justice of the European Union in its Schrems judgment. The court held that the European Commission decision underlying Safe Harbor did not ensure an adequate level of protection for personal data transferred from the European Union to the United States. In particular, the framework did not sufficiently limit or provide effective legal remedies concerning U.S. public-authority access to transferred data. Consequently, organizations could no longer rely on a Safe Harbor self-certification to lawfully transfer personal data under the EU data-transfer regime.

GDPR Chapter V requires a transfer to a third country to comply with one of its recognized transfer conditions. The European Commission's current adequacy framework for participating U.S. organizations is the EU-U.S. Data Privacy Framework, adopted in 2023; this is legally distinct from the former Safe Harbor Framework. Therefore, a reference to Safe Harbor identifies an obsolete and invalid transfer arrangement, rather than a lawful basis for a present-day transfer. See the Court of Justice press release on Schrems and the European Commission's adequacy decisions overview.

## QUESTION NO: 8

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.

**ANSWER: A**

**Explanation:**

The affected individuals must be informed when significant harm is likely to occur. Under Singapore's Personal Data Protection Act, an organisation that assesses a data breach as notifiable must notify affected individuals if the breach is likely to result in significant harm to them. This notification must be made at the same time as, or after, notification to the Personal Data Protection Commission, and it must be made as soon as practicable. The individual notice should contain sufficient information for a person to understand the breach and take protective steps, such as changing credentials or watching for fraud. Significant harm may arise, for example, where compromised data could facilitate identity theft, financial loss, or other serious adverse consequences. This statutory, individual-focused notification obligation gives Singapore residents a direct mechanism to learn of serious incidents affecting their personal data and respond to the associated risk. Singapore's PDPC explains the assessment and notification duties in its data-breach guidance; the underlying requirements appear in the Personal Data Protection Act 2012, Part VIA.

**QUESTION NO: 9**

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.

**ANSWER: A**

**Explanation:**

It expanded the interpretation of right to life under Article 21 of the Constitution. In *Maneka Gandhi v. Union of India*, the Supreme Court gave Article 21 a transformative reading by holding that a person cannot be deprived of life or personal liberty through merely any procedure enacted by legislation. The procedure must be "right, just and fair," and cannot be arbitrary, fanciful, or oppressive. The Court also read Articles 14, 19, and 21 together, meaning that a law affecting personal liberty must satisfy equality and relevant freedom protections as well as Article 21's procedural safeguard. This substantially changed Indian constitutional law from a narrow, formal view of legally prescribed procedure to a rights-protective review of the fairness and reasonableness of state action. That approach became the foundation for later recognition of a broad range of Article 21 protections, including dignity, autonomy, livelihood-related interests, and procedural fairness. The judgment is therefore especially significant because it established the doctrinal basis for an expansive understanding of life and personal liberty under the Constitution. See the full decision at Indian Kanoon: Maneka Gandhi v. Union of India and the Supreme Court of India's constitutional framework at Supreme Court of India: Constitution of India.

**QUESTION NO: 10**

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.

**ANSWER: D**

**Explanation:**

The patient can buy medications from Bharat Medicals by uploading prescription to the Bharat Medicals website. Withdrawal of consent given to the hospital concerns the hospital's further transfer of the patient's treatment and order information to Bharat Medicals. It does not prevent the patient from independently using Bharat Medicals' e-commerce service. The scenario expressly provides a separate ordering route: a registered consumer may place an order through the website and, where required, upload the prescription authorization. That submission is made directly by the patient, or by a person authorized by the patient, under the privacy notice presented during registration.

Under India's Sensitive Personal Data or Information Rules, a data provider may withdraw previously given consent. The body corporate may then decide not to provide the particular goods or services for which that consent was necessary, but the withdrawal does not automatically eliminate unrelated service channels or prohibit the individual from providing information directly for a new transaction. Here, direct website ordering is operationally and legally distinct from the hospital-to-retailer data-transfer arrangement. See Rule 5(7) of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and the Information Technology Act, 2000.

**QUESTION NO: 11**

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.

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.

**ANSWER: D**

**Explanation:**

Yes, if the research is deemed to be in the public interest. Singapore's Personal Data Protection Act provides a consent exception for use of personal data for a research purpose where specified safeguards are met. In particular, the research must not reasonably be achievable without using personal data in identifiable form, and a reasonable person must consider that the public benefit of the research clearly outweighs any adverse effect on the individual. The organization must also comply with applicable conditions that protect the individual and limit the handling of the data to the permitted research purpose.

Accordingly, Carl's departure from employment and the absence of fresh consent do not automatically prevent the proposed research. B-Star may rely on the research exception only where the statutory public-benefit assessment and associated requirements are actually satisfied; "public interest" is not simply an internal business preference or a general claim of usefulness. This approach reflects the PDPA's balance between meaningful consent and carefully defined exceptions that permit socially beneficial research while retaining protections for identifiable personal data. The relevant exception is set out in Singapore's Second Schedule to the Personal Data Protection Act 2012; see also the PDPC's PDPA legislation overview.

**QUESTION NO: 12**

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.

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.

**ANSWER: C**

**Explanation:**

Inform the staff that Relax Ltd should not transfer the data to StarOne without the guest's opt-in consent to do so. Relax Ltd is an independently owned business and is therefore responsible for ensuring that its disclosure of spa guests' personal data complies with Hong Kong's Personal Data (Privacy) Ordinance. A guest's provision of information to Relax Ltd for spa services does not, by itself, establish permission for Relax Ltd to disclose that information to StarOne for StarOne's own systems and handling. Such a disclosure must be within the purpose for which the data was collected, or a directly related purpose, unless the guest has given prescribed consent for a new purpose. In this setting, appropriately obtained opt-in consent provides the clearest basis for the proposed sharing: it should be voluntary, express, informed, and recorded, and guests should understand that their spa data will be transferred to StarOne for storage and related administration. The Privacy Commissioner explains that Data Protection Principle 3 limits use of personal data to the collection purpose or a directly related purpose, with prescribed consent required for a new purpose. The statutory definition of prescribed consent also requires consent to be given voluntarily and expressly. See the PCPD's overview of the Ordinance and Cap. 486, Personal Data (Privacy) Ordinance.