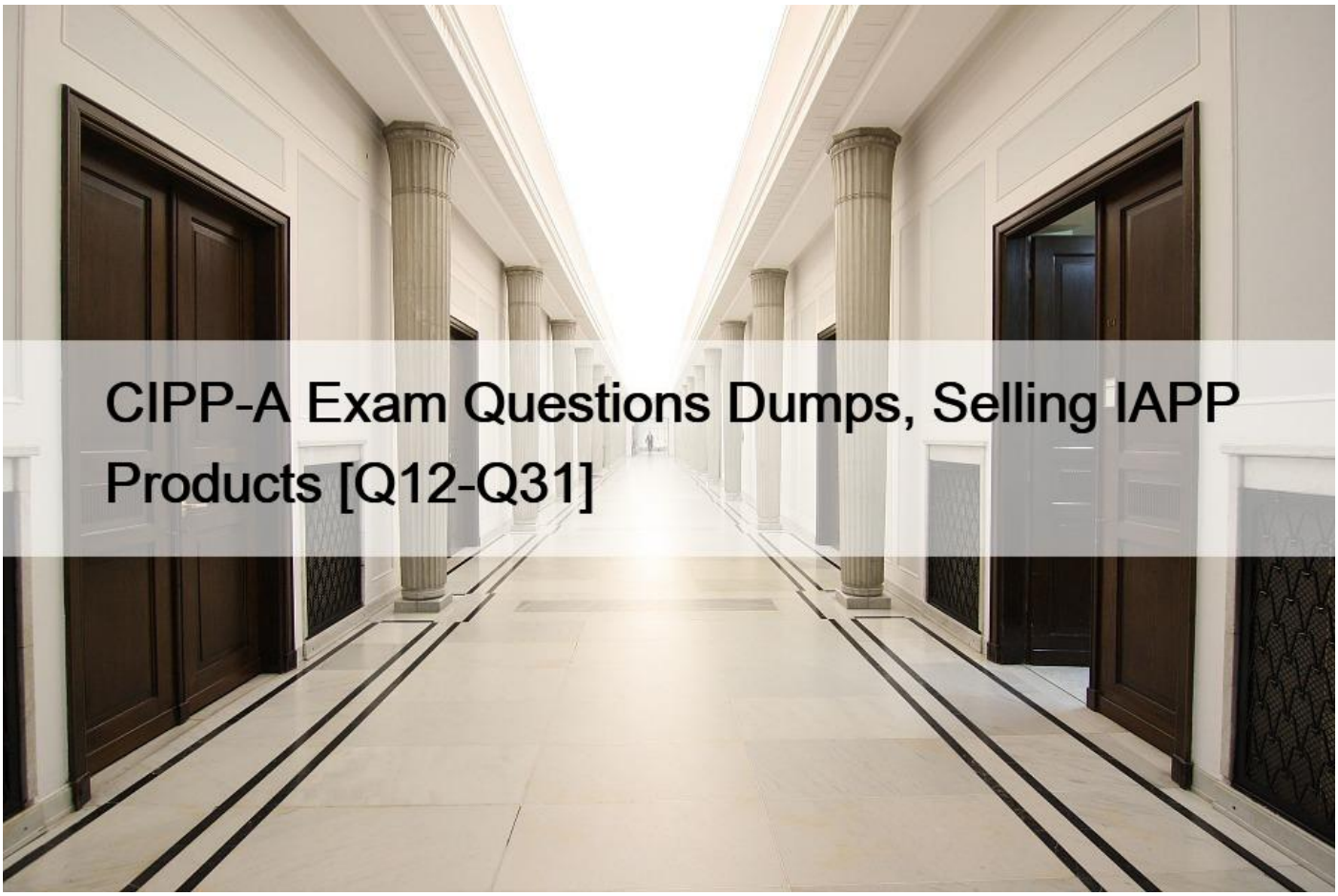
CIPP-A Exam Questions Dumps, Selling IAPP Products [Q12-Q31



CIPP-A Exam Questions Dumps, Selling IAPP Products
CIPP-A Cert Guide PDF 100% Cover Real Exam Questions

Q12. 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 Chin a. 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.

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

Q13. 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.

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?

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

Q14. Which of the following is NOT a way that the Singapore government can monitor its citizens?
* Through the national identity card system.
* Through the electronic road pricing system.
* Through a personal computer registration system.
* Through an online service that holds an individual’s medical records.

Q15. Hong Kong’s definition of a data user in the original PDPO applies to all of the following EXCEPT?
* Trust corporations.
* Third-party processors.
* Private sector organizations.
* Limited liability partnerships.

Q16. Which of the following is NOT excluded from the scope of Singapore’s Do Not Call registry?
* Messages that promote investment opportunities.
* Messages that conduct market research.
* Messages from charitable organizations.
* Messages from political candidates.

Q17. In India, the obligation to appoint a Grievance Officer applies ONLY to companies that?
* Deal with sensitive personal data.
* Conduct cross-border data transfers.
* Are considered part of the public sector.
* Lack alternate enforcement mechanisms.

Reference:

https://taxguru.in/corporate-law/compliance-relation-appointment-grievance-officer-provisions-information-technology-act-2000.html

Q18. Increases in which of the following were a major reason for the enactment of Hong Kong’s Amendment Ordinance in 2012?
* Law enforcement requests.
* Biometric authentication.
* Direct marketing practices.
* Data breach reports.

Q19. 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.

Dracarys and their vendor of choice must draft a contract that establishes agreement regarding all of the following factors EXCEPT?
* Breach notification.
* Data retention periods.
* Employee recruitment process.
* Data subject consent provisions.

Q20. According to India’s IT Rules 2011, a body corporate operating in India is required to appoint what kind of authority?
* A Chief Risk Officer.
* A Grievance Officer.
* A Data Protection Officer.
* A Chief Technology Officer.

Q21. Under the PDPO, what are Hong Kong companies that make use of personal data required to do?
* Appoint an official compliance officer.
* Register with the appropriate data authority.
* Honor all data subject requests for correcting personal information.
* Provide contact information of persons handling data access requests.

Q22. What benefit does making data pseudonymous offer to data controllers?
* It ensures that it is impossible to re-identify the data.
* It eliminates the responsibility to report data breaches.
* It allows for further use of the data for research purposes.
* It eliminates the need for a policy specifying data subject access rights.

Q23. 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?
* No, because Jimmy is not in the division that Bigbank seeks to acquire.
* No, because the data was collected for the express purpose of complying with Singabank’s privacy policies.
* Yes, if Singabank informs Jimmy of the disclosure of his personal data before it occurs.
* Yes, if Jimmy’s personal data is necessary for Bigbank to determine whether to proceed with the acquisition.

Q24. What emerged as the main reason for creating a comprehensive data protection law when Singapore ministers met between 2005 and 2011?
* To control increasing technological threats.
* To raise Singapore’s human rights standing.
* To limit the scope of governmental surveillance.
* To enhance Singapore’s economic competitiveness.

Q25. Which of the following does Singapore’s PDPC NOT have the power to do?
* Order an organization to stop collecting personal data.
* Order an organization to destroy collected personal data.
* Order an organization to award compensation to a complainant.
* Order an organization to pay a financial penalty to the government.

Q26. Section 43A of India’s IT Rules 2011 requires which of the following for a privacy policy?
* It should be available and produced on request.
* It should be published on the website of the body corporate.
* It should be emailed or faxed to data providers by the body corporate.
* It should be shown to the data provider at the time of data collection.

Reference:

rules-2011-

Q27. In which of the following cases would a Singaporean be prevented from accessing information about herself from an organization?
* The information was collected in the previous 12 months.
* The information is related to an individual’s credit rating.
* The cost of providing the information proved to be unreasonable.
* Any personal information about others has been deleted from the document.

Q28. In what way are Hong Kong citizens protected from direct marketing in ways that India and Singapore citizens are not?
* Subscribers must have explicitly indicated that they did not object to their data being collected and used for marketing purposes.
* Subscribers can opt out of the use of their data for marketing purposes after collection by withdrawing consent.
* Data subjects must be notified on a website if their data is being used for marketing purposes.
* Data subjects are protected from the secondary use of personal data for marketing purposes.

Q29. 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 Indi a. 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?
* The patient cannot purchase medications from Bharat Medicals.
* The hospital has the right to refuse withdrawal of consent since it has a partnership with Bharat Medicals.
* The hospital will obtain the necessary medications from Bharat Medicals and provide them directly to patient.
* The patient can buy medications from Bharat Medicals by uploading prescription to the Bharat Medicals website.

Q30. 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 Asi a. 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 practices would likely violate Hong Kong’s Data Protection Principle 1 regarding data collection?
* FFE’s collection of full name from prospective clients.
* FFE affiliates’ receipt of Stephen’s contact information.
* FFE’s collection of age and HKID from prospective clients.
* FFE’s collection of Stephen’s messenger cell details through Kelvin.

Q31. Which of the following principles of the OECD guidelines and Council of European Convention principles does Singapore’s PDPA incorporate?
* Disclosures to third parties included in access requests.
* Additional protections for sensitive personal data.
* The ability to opt-out from direct marketing.
* The right of deletion of data on request.