CIPM$^{Q\&As}$

Certified Information Privacy Manager

Pass IAPP CIPM Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/cipm.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by IAPP Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Under the General Data Protection Regulation (GDPR), what obligation does a data controller or processor have after appointing a Data Protection Officer (DPO)?

A. To submit for approval to the DPO a code of conduct to govern organizational practices and demonstrate compliance with data protection principles.

B. To provide resources necessary to carry out the defined tasks of the DPO and to maintain their expert knowledge.

C. To ensure that the DPO acts as the sole point of contact for individuals' questions about their personal data.

D. To ensure that the DPO receives sufficient instructions regarding the exercise of their defined tasks.

Correct Answer: B

QUESTION 2

Why were the nongovernmental privacy organizations, Electronic Frontier Foundation (EFF) and Electronic Privacy Information Center (EPIC), established?

A. To promote consumer confidence in the Internet industry.

B. To improve the user experience during online shopping.

C. To protect civil liberties and raise consumer awareness.

D. To promote security on the Internet through strong encryption.

Correct Answer: C

Reference: https://en.wikipedia.org/wiki/Electronic_Privacy_Information_Center

QUESTION 3

Which statement is FALSE regarding the use of technical security controls?

A. Technical security controls are part of a data governance strategy.

B. Technical security controls deployed for one jurisdiction often satisfy another jurisdiction.

C. Most privacy legislation lists the types of technical security controls that must be implemented.

D. A person with security knowledge should be involved with the deployment of technical security controls.

Correct Answer: B

QUESTION 4

SCENARIO

Please use the following to answer the next QUESTION:

John is the new privacy officer at the prestigious international law firm ?and;M LLP. and;M LLP is very proud of its reputation in the practice areas of Trusts and Estates and Merger and Acquisition in both U.S. and Europe.

During lunch with a colleague from the Information Technology department, John heard that the Head of IT, Derrick, is about to outsource the firm\\'s email continuity service to their existing email security vendor ?MessageSafe. Being

successful as an email hygiene vendor, MessageSafe is expanding its business by leasing cloud infrastructure from Cloud Inc. to host email continuity service for AandM LLP.

John is very concerned about this initiative. He recalled that MessageSafe was in the news six months ago due to a security breach. Immediately, John did a quick research of MessageSafe\\'s previous breach and learned that the breach was

caused by an unintentional mistake by an IT administrator. He scheduled a meeting with Derrick to address his concerns.

At the meeting, Derrick emphasized that email is the primary method for the firm\\'s lawyers to communicate with clients, thus it is critical to have the email continuity service to avoid any possible email downtime. Derrick has been using the

anti-spam service provided by MessageSafe for five years and is very happy with the quality of service provided by MessageSafe. In addition to the significant discount offered by MessageSafe, Derrick emphasized that he can also speed up

the onboarding process since the firm already has a service contract in place with MessageSafe. The existing on-premises email continuity solution is about to reach its end of life very soon and he doesn\\'t have the time or resource to look for

another solution. Furthermore, the off-premises email continuity service will only be turned on when the email service at AandM LLP\\'s primary and secondary data centers are both down, and the email messages stored at MessageSafe site for

continuity service will be automatically deleted after 30 days.

Which of the following is the most effective control to enforce MessageSafe\\'s implementation of appropriate technical countermeasures to protect the personal data received from AandM LLP?

A. MessageSafe must apply due diligence before trusting Cloud Inc. with the personal data received from AandM LLP.

B. MessageSafe must flow-down its data protection contract terms with AandM LLP to Cloud Inc.

C. MessageSafe must apply appropriate security controls on the cloud infrastructure.

D. MessageSafe must notify AandM LLP of a data breach.

Correct Answer: D

QUESTION 5

SCENARIO

Please use the following to answer the next QUESTION:

Martin Briseno is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseno decided to change the hotel\\'s on-the-job mentoring model to a standardized training program for employees who were progressing from line positions into supervisory positions. He developed a curriculum comprising a series of lessons, scenarios, and assessments, which was delivered in-person to small groups. Interest in the training increased, leading Briseno to work with corporate HR specialists and software engineers to offer the program in an online format. The online program saved the cost of a trainer and allowed participants to work through the material at their own pace.

Upon hearing about the success of Briseno\\'s program, Pacific Suites corporate Vice President Maryanne Silva-Hayes expanded the training and offered it company-wide. Employees who completed the program received certification as a Pacific Suites Hospitality Supervisor. By 2001, the program had grown to provide industry-wide training. Personnel at hotels across the country could sign up and pay to take the course online. As the program became increasingly profitable, Pacific Suites developed an offshoot business, Pacific Hospitality Training (PHT). The sole focus of PHT was developing and marketing a variety of online courses and course progressions providing a number of professional certifications in the hospitality industry.

By setting up a user account with PHT, course participants could access an information library, sign up for courses, and take end-of-course certification tests. When a user opened a new account, all information was saved by default, including the user\\'s name, date of birth, contact information, credit card information, employer, and job title. The registration page offered an opt-out choice that users could click to not have their credit card numbers saved. Once a user name and password were established, users could return to check their course status, review and reprint their certifications, and sign up and pay for new courses. Between 2002 and 2008, PHT issued more than 700,000 professional certifications.

PHT\\'s profits declined in 2009 and 2010, the victim of industry downsizing and increased competition from e- learning providers. By 2011, Pacific Suites was out of the online certification business and PHT was dissolved. The training program\\'s systems and records remained in Pacific Suites\\' digital archives, un-accessed and unused. Briseno and Silva- Hayes moved on to work for other companies, and there was no plan for handling the archived data after the program ended. After PHT was dissolved, Pacific Suites executives turned their attention to crucial day-to-day operations. They planned to deal with the PHT materials once resources allowed.

In 2012, the Pacific Suites computer network was hacked. Malware installed on the online reservation system exposed the credit card information of hundreds of hotel guests. While targeting the financial data on the reservation site, hackers also discovered the archived training course data and registration accounts of Pacific Hospitality Training\\'s customers. The result of the hack was the exfiltration of the credit card numbers of recent hotel guests and the exfiltration of the PHT database with all its contents.

A Pacific Suites systems analyst discovered the information security breach in a routine scan of activity reports. Pacific Suites quickly notified credit card companies and recent hotel guests of the breach, attempting to prevent serious harm. Technical security engineers faced a challenge in dealing with the PHT data.

PHT course administrators and the IT engineers did not have a system for tracking, cataloguing, and storing information. Pacific Suites has procedures in place for data access and storage, but those procedures were not implemented when PHT was formed. When the PHT database was acquired by Pacific Suites, it had no owner or oversight. By the time technical security engineers determined what private information was compromised, at least 8,000 credit card holders were potential victims of fraudulent activity. What must Pacific Suite\\'s primary focus be as it manages this security breach?

A. Minimizing the amount of harm to the affected individuals

B. Investigating the cause and assigning responsibility

C. Determining whether the affected individuals should be notified

D. Maintaining operations and preventing publicity

Correct Answer: A