Free Questions for CIPM

Shared by Lancaster on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SCENARIO

Please use the following to answer the next QUESTION:

Martin Briseo is the director of human resources at the Canyon City location of the U.S. hotel chain Pacific Suites. In 1998, Briseo 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 Briseo 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 Briseo'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. Briseo 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.

In the Information Technology engineers had originally set the default for customer credit card information to ''Do Not Save,'' this action would have been in line with what concept?

Options:

A- Use limitation
B- Privacy by Design
C- Harm minimization
D- Reactive risk management

Answer:

B

Question 2

Question Type: MultipleChoice

While trying to e-mail her manager, an employee has e-mailed a list of all the company's customers, including their bank details, to an employee with the same name at a different company. Which of the following would be the first stage in the incident response plan under the General Data Protection Regulation (GDPR)?

Options:

A- Notification to data subjects.
B- Containment of impact of breach.

C- Remediation offers to data subjects.
D- Notification to the Information Commissioner's Office (ICO).

Answer:

B

Explanation:

The first stage in the incident response plan under the General Data Protection Regulation (GDPR) for this scenario would be to contain the impact of the breach. This means taking immediate action to stop the unauthorized access or disclosure of personal data, and to prevent it from happening again in the future. This could involve revoking access to the data, notifying the employee who mistakenly sent the data, and implementing security measures to prevent similar breaches from occurring in the future.

https://gdpr-info.eu/art-33-gdpr/

https://gdpr-info.eu/art-34-gdpr/

Question 3

Question Type: MultipleChoice

SCENARIO

Please use the following to answer the next QUESTION:

Your organization, the Chicago (U.S.)-based Society for Urban Greenspace, has used the same vendor to operate all aspects of an online store for several years. As a small nonprofit, the Society cannot afford the higher-priced options, but you have been relatively satisfied with this budget vendor, Shopping Cart Saver (SCS). Yes, there have been some issues. Twice, people who purchased items from the store have had their credit card information used fraudulently subsequent to transactions on your site, but in neither case did the investigation reveal with certainty that the Society's store had been hacked. The thefts could have been employee-related.

Just as disconcerting was an incident where the organization discovered that SCS had sold information it had collected from customers to third parties. However, as Jason Roland, your SCS account representative, points out, it took only a phone call from you to clarify expectations and the ''misunderstanding'' has not occurred again.

As an information-technology program manager with the Society, the role of the privacy professional is only one of many you play. In all matters, however, you must consider the financial bottom line. While these problems with privacy protection have been significant, the

additional revenues of sales of items such as shirts and coffee cups from the store have been significant. The Society's operating budget is slim, and all sources of revenue are essential.

Now a new challenge has arisen. Jason called to say that starting in two weeks, the customer data from the store would now be stored on a data cloud. ''The good news,'' he says, ''is that we have found a low-cost provider in Finland, where the data would also be held. So, while there may be a small charge to pass through to you, it won't be exorbitant, especially considering the advantages of a cloud.''

Lately, you have been hearing about cloud computing and you know it's fast becoming the new paradigm for various applications. However, you have heard mixed reviews about the potential impacts on privacy protection. You begin to research and discover that a number of the leading cloud service providers have signed a letter of intent to work together on shared conventions and technologies for privacy protection. You make a note to find out if Jason's Finnish provider is signing on.

What is the best way to prevent the Finnish vendor from transferring data to another party?

Options:

A- Restrict the vendor to using company security controls
B- Offer company resources to assist with the processing
C- Include transfer prohibitions in the vendor contract
D- Lock the data down in its current location

Answer:

C

Explanation:

This answer is the best way to prevent the Finnish vendor from transferring data to another party, as it can establish clear and binding terms and conditions for both parties regarding their roles and responsibilities for data processing activities. Including transfer prohibitions in the vendor contract can help to define the scope, purpose, duration and type of data processing, as well as the rights and obligations of both parties. The contract can also specify that the vendor is not allowed to share, disclose or transfer the data to any third party without the prior consent or authorization of the organization, and that any breach of this clause may result in legal actions, penalties or termination of the contract.

Question 4

Question Type: MultipleChoice

SCENARIO

Please use the following to answer the next QUESTION:

Penny has recently joined Ace Space, a company that sells homeware accessories online, as its new privacy officer. The company is based in California but thanks to some great publicity from a social media influencer last year, the company has received an influx of sales from the EU and has set up a regional office in Ireland to support this expansion. To become familiar with Ace Space's practices and assess what her privacy priorities will be, Penny has set up meetings with a number of colleagues to hear about the work that they have been doing and their compliance efforts.

Penny's colleague in Marketing is excited by the new sales and the company's plans, but is also concerned that Penny may curtail some of the growth opportunities he has planned. He tells her ''I heard someone in the breakroom talking about some new privacy laws but I really don't think it affects us. We're just a small company. I mean we just sell accessories online, so what's the real risk?'' He has also told her that he works with a number of small companies that help him get projects completed in a hurry. ''We've got to meet our deadlines otherwise we lose money. I just sign the contracts and get Jim in finance to push through the payment. Reviewing the contracts takes time that we just don't have.''

In her meeting with a member of the IT team, Penny has learned that although Ace Space has taken a number of precautions to protect its website from malicious activity, it has not taken the same level of care of its physical files or internal infrastructure. Penny's colleague in IT has told her that a former employee lost an encrypted USB key with financial data on it when he left. The company nearly lost access to their customer database last year after they fell victim to a phishing attack. Penny is told by her IT colleague that the IT team ''didn't know what to do or who should do what. We hadn't been trained on it but we're a small team though, so it worked out OK in the end.'' Penny is concerned that these issues will compromise Ace Space's privacy and data protection.

Penny is aware that the company has solid plans to grow its international sales and will be working closely with the CEO to give the organization a data ''shake up''. Her mission is to cultivate a strong privacy culture within the company.

Penny has a meeting with Ace Space's CEO today and has been asked to give her first impressions and an overview of her next steps.

What is the best way for Penny to understand the location, classification and processing purpose of the personal data Ace Space has?

Options:

A- Analyze the data inventory to map data flows
B- Audit all vendors' privacy practices and safeguards
C- Conduct a Privacy Impact Assessment for the company
D- Review all cloud contracts to identify the location of data servers used

Answer:

A

Explanation:

The best way for Penny to understand the location, classification and processing purpose of the personal data Ace Space has is to analyze the data inventory to map data flows. A data inventory is a comprehensive record of the personal data that an organization collects, stores, uses and shares. It helps to identify the sources, categories, locations, recipients and retention periods of personal data. A data flow map is a visual representation of how personal data flows within and outside an organization. It helps to identify the data transfers, processing activities, legal bases, risks and safeguards of personal data.

By analyzing the data inventory and mapping the data flows, Penny can gain a clear picture of the personal data lifecycle at Ace Space and identify any gaps or issues that need to be addressed. For example, she can determine whether Ace Space has a lawful basis for processing personal data of EU customers, whether it has adequate security measures to protect personal data from unauthorized access or loss, whether it has appropriate contracts with its vendors and cloud providers to ensure compliance with applicable laws and regulations, and whether it has mechanisms to respect the rights and preferences of its customers.

The other options are not the best way for Penny to understand the location, classification and processing purpose of the personal data Ace Space has. Auditing all vendors' privacy practices and safeguards (B) is an important step to ensure that Ace Space's third-party processors are complying with their contractual obligations and legal requirements, but it does not provide a comprehensive overview of Ace Space's own personal data processing activities. Conducting a Privacy Impact Assessment (PIA) for the company is a useful tool to assess the privacy risks and impacts of a specific project or initiative involving personal data, but it does not provide a baseline understanding of the existing personal data landscape at Ace Space. Reviewing all cloud contracts to identify the location of data servers used (D) is a relevant aspect of understanding the location of personal data, but it does not cover other aspects such as classification and processing purpose.

CIPM Body of Knowledge Domain I: Privacy Program Governance - Task 1: Establish privacy program vision and strategy - Subtask 1: Identify applicable privacy laws, regulations and standards

CIPM Body of Knowledge Domain II: Privacy Program Operational Life Cycle - Task 1: Assess current state of privacy in an organization - Subtask 1: Conduct gap analysis

CIPM Study Guide - Chapter 2: Privacy Program Governance - Section 2.1: Data Inventory

CIPM Study Guide - Chapter 2: Privacy Program Governance - Section 2.2: Data Flow Mapping

Question 5

Question Type: MultipleChoice

What is least likely to be achieved by implementing a Data Lifecycle Management (DLM) program?

Options:

A- Reducing storage costs.
B- Ensuring data is kept for no longer than necessary.
C- Crafting policies which ensure minimal data is collected.
D- Increasing awareness of the importance of confidentiality.

Answer:

C

Explanation:

Crafting policies which ensure minimal data is collected is least likely to be achieved by implementing a Data Lifecycle Management (DLM) program, as it is more related to the data collection stage, not the data management stage. A DLM program focuses on how to handle the data after it has been collected, such as how to store, use, share, and dispose of it. The other options are more likely to be achieved by implementing a DLM program, as they help to optimize the data storage costs, comply with the data retention obligations, and protect the data confidentiality.Reference:CIPM Body of Knowledge, Domain III: Privacy Program Management Activities, Task 1: Manage data inventory.

Question 6

Question Type: MultipleChoice

Under the General Data Protection Regulation (GDPR), when would a data subject have the right to require the erasure of his or her data without undue delay?

Options:

A- When the data subject is a public authority.
B- When the erasure is in the public interest.
C- When the processing is carried out by automated means.
D- When the data is no longer necessary for its original purpose.

Answer:

D

Explanation:

This answer is one of the situations when a data subject would have the right to require the erasure of his or her data without undue delay under the General Data Protection Regulation (GDPR), which is also known as the right to be forgotten or the right to erasure. This right allows a data subject to request that a data controller deletes his or her personal data when one of the following grounds applies:

The data is no longer necessary for its original purpose.

The data subject withdraws his or her consent for processing.

The data subject objects to processing based on legitimate interests or direct marketing.

The processing is unlawful or violates other laws or regulations.

The processing is related to online services offered to children.