Free Questions for CIPM by dumpshq

Shared by Phelps on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is a physical control that can limit privacy risk?

Options:

A- Keypad or biometric access.

B- user access reviews.

C- Encryption.

D- Tokenization.

Answer:

A

Explanation:

A physical control that can limit privacy risk is keypad or biometric access. This is a type of access control that restricts who can enter or access a physical location or device where personal data is stored or processed. Keypad or biometric access requires a code or a biological feature (such as a fingerprint or a face scan) to authenticate the identity and authorization of the person seeking access. This

can prevent unauthorized access, theft, loss, or damage of personal data by outsiders or insiders, .Reference:[CIPM - International Association of Privacy Professionals], [Free CIPM Study Guide - International Association of Privacy Professionals]

Question 2

Question Type: MultipleChoice

Under the GDPR. when the applicable lawful basis for the processing of personal data is a legal obligation with which the controller must comply. which right can the data subject exercise?

Options:

A- Right to withdraw consent.

B- Right to data portability.

C- Right to restriction.

D- Right to erasure.

Answer:

C

Explanation:

Under the GDPR, when the applicable lawful basis for the processing of personal data is a legal obligation with which the controller must comply, the data subject can exercise the right to restriction. This means that the data subject can request the controller to limit the processing of their personal data in certain circumstances, such as when they contest the accuracy or lawfulness of the processing. The other rights are not applicable in this case, as they are either dependent on consent (right to withdraw consent and right to data portability) or subject to exceptions (right to erasure).Reference:GDPR, Articles 6(1), 18, 21(1).

Question 3

Question Type: MultipleChoice

Integrating privacy requirements into functional areas across the organization happens at which stage of the privacy operational life cycle?

Options:

A- Assessing data.

B- Protecting personal data.

C- Sustaining program performance.

D- Responding to requests and incidents.

Answer:

B

Explanation:

Integrating privacy requirements into functional areas across the organization happens at the "protect" stage of the privacy operational life cycle. This stage involves implementing privacy policies, procedures, and controls to ensure that personal data is processed in a lawful, fair, and transparent manner. The other stages of the privacy operational life cycle are "assess", "align", "respond", and "sustain".Reference:CIPM Body of Knowledge, Domain III: Privacy Program Operational Life Cycle, Section B: Protect.

Question 4

Question Type: MultipleChoice

Which of the following is NOT a main technical data control area?

Options:

A- Obfuscation.

B- Tokenization.

C- Access controls.

D- Data minimization.

Answer:

A

Explanation:

Obfuscation is not a main technical data control are

a. Obfuscation means hiding or disguising data or information to make it less intelligible or accessible. Obfuscation can be used as a security measure or a privacy-enhancing technique, but it is not a specific type of data control. The main technical data control areas are tokenization, encryption, access controls, and data minimization. Tokenization means replacing sensitive data with non-sensitive substitutes called tokens that have no intrinsic value. Encryption means transforming data into an unreadable format that can only be decrypted with a key. Access controls mean restricting who can access or modify data based on their roles, permissions, or authentication methods.Data minimization means collecting, storing, and processing only the minimum amount of data necessary for a specific purpose1,2.Reference:CIPM - International Association of Privacy Professionals,Free CIPM Study Guide - International Association of Privacy Professionals

Question 5

Question Type: MultipleChoice

When a data breach incident has occurred. the first priority is to determine?

Options:

A- Who caused the breach.

B- How the breach occurred.

C- How to contain the breach.

D- When the breach occurred.

Answer:

C

Explanation:

When a data breach incident has occurred, the first priority is to determine how to contain the breach. Containment means stopping or minimizing the further loss or unauthorized disclosure of personal data, as well as preserving evidence for investigation and remediation. Containment may involve isolating affected systems, devices, or networks; changing access credentials; blocking malicious IP addresses; or notifying relevant parties such as law enforcement or security experts.After containing the breach, the next steps are to assess the impact and severity of the breach, notify the affected individuals and authorities if required, evaluate the causes and risks of the breach, and implement measures to prevent future breaches1,2.Reference:CIPM - International Association of Privacy Professionals,Free CIPM Study Guide - International Association of Privacy Professionals

Question 6

Question Type: MultipleChoice

Your company provides a SaaS tool for B2B services and does not interact with individual consumers. A client's current employee reaches out with a right to delete request. what is the most appropriate response?

Options:

A- Forward the request to the contact on file for the client asking them how they would like you to proceed.

B- Redirect the individual back to their employer to understand their rights and how this might impact access to company tools.

C- Process the request assuming that the individual understands the implications to their organization if their information is deleted.

D- Explain you are unable to process the request because business contact information and associated data is not covered under privacy rights laws.

Answer:

B

Explanation:

If your organization provides a SaaS tool for B2B services and does not interact with individual consumers, and a client's current employee reaches out with a right to delete request, the most appropriate response is to redirect the individual back to their employer to understand their rights and how this might impact access to company tools. This is because your organization is acting as a processor for the client, who is the controller of the employee's personal dat

a. The controller is responsible for determining the purposes and means of processing personal data, as well as responding to data subject requests. The processor should only process personal data on behalf of and in accordance with the instructions of the controller.Therefore, you should not forward the request to the client, process the request without consulting the client, or deny the request based on business contact information being exempt from privacy rights laws1,2.Reference:CIPM - International Association of Privacy Professionals,Free CIPM Study Guide - International Association of Privacy Professionals

Question 7

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 for your vendor to be clear about the Society's breach notification expectations?

Options:

A- Include notification provisions in the vendor contract

B- Arrange regular telephone check-ins reviewing expectations

C- Send a memorandum of understanding on breach notification

D- Email the regulations that require breach notifications

Answer:

A

Explanation:

This answer is the best way for Albert's vendor to be clear about the Society's breach notification expectations, as it can establish clear and binding terms and conditions for both parties regarding their roles and responsibilities for handling any data security incidents or breaches. Including notification provisions in the vendor contract can help to define what constitutes a breach, how it should be detected,

reported and investigated, what information should be provided to the organization and within what time frame, what actions should be taken to mitigate or resolve the breach, and what consequences or liabilities may arise from the breach. The contract can also specify that the vendor must cooperate and coordinate with the organization in any breach notification activities to the relevant authorities, customers, partners or stakeholders.

Question 8

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 process can best answer your Questions about the vendor's data security safeguards?

Options:

A- A second-party of supplier audit

B- A reference check with other clients

C- A table top demonstration of a potential threat

D- A public records search for earlier legal violations

Answer:

A

Explanation:

This answer is the best process to answer Albert's questions about the vendor's data security safeguards, as it can provide a direct and comprehensive way to assess and verify the vendor's compliance with the applicable laws, regulations, standards and best practices for data protection. A second-party or supplier audit is conducted by the organization that hires or contracts the vendor to evaluate their performance and alignment with the organization's standards and expectations. A second-party or supplier audit can also help to identify any gaps, weaknesses or risks in the vendor's data security safeguards, and to recommend or require any improvements or corrective actions.

Question 9

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.