Free Questions for CIPT by certsinside

Shared by Solomon on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

In terms of data extraction, which of the following should NOT be considered by a privacy technologist in relation to data portability?

Options:

A- The size of the data.

B- The format of the data.

C- The range of the data.

D- The medium of the data.

Answer:

D

Explanation:

The medium of the data. Data portability refers to an individual's right to receive their personal data in a structured and commonly used format so that they can transfer it to another service provider. The size (A), format (B), and range of the data are all relevant considerations when extracting data for portability purposes. However, the medium of the data is not relevant in this context.

Question 2

Question Type: MultipleChoice

When writing security policies, the most important consideration is to?

Options:

A- Require all employees to read and acknowledge their understanding.

B- Ensure they are based on the organization's risk profile.

C- Ensure they cover enough details for common situations.

D- Follow industry best practices.

Answer:

B

Explanation:

the most important consideration when writing security policies is to ensure they are based on the organization's risk profile. This means that the policies should be tailored to address the specific risks faced by the organization.

Question 3

Question Type: MultipleChoice

A BaaS provider backs up the corporate data and stores it in an outsider provider under contract with the organization. A researcher notifies the organization that he found unsecured data in the cloud. The organization looked into the issue and realized $ne of its backups was misconfigured on the outside provider's cloud and the data fully exposed to the open internet. They quickly secured the backup. Which is the best next step the organization should take?

Options:

A- Review the content of the data exposed.

B- Review its contract with the outside provider.

C- Investigate how the researcher discovered the unsecured data.

D- Investigate using alternate BaaS providers or on-premise backup systems.

Answer:

B

Explanation:

The best next step the organization should take is toreview its contract with the outside provider. This will help the organization to identify the responsibilities of the outside provider and the organization in the event of a data breach.

Question 4

Question Type: MultipleChoice

An organization must terminate their cloud vendor agreement immediately. What is the most secure way to delete the encrypted data stored in the cloud?

Options:

A- Transfer the data to another location.

B- Invoke the appropriate deletion clause in the cloud terms and conditions.

C- Obtain a destruction certificate from the cloud vendor.

D- Destroy all encryption keys associated with the data.

Answer:

D

Explanation:

Destroying all encryption keys associated with encrypted data stored on a cloud server would make that encrypted data inaccessible even if it still exists on that server4.

Question 5

Question Type: MultipleChoice

Which of the following is a stage in the data life cycle?

Options:

A- Data classification.

B- Data inventory.

C- Data masking.

D- Data retention.

Answer:

D

Explanation:

The stages in a typical data lifecycle include creation/collection, processing, storage/retention, usage/access/sharing/distribution, archival/preservation and destruction/deletion/disposition3. Among these options provided here only "Data retention" is a stage in this cycle.

Question 6

Question Type: MultipleChoice

Which of the following is most important to provide to the data subject before the collection phase of the data lifecycle?

Options:

A- Privacy Notice.

B- Disclosure Policy.

C- Consent Request.

D- Data Protection Policy.

Answer:

A

Explanation:

A Privacy Notice is important to provide to data subjects before collecting their personal data because it informs them about how their data will be used, who it will be shared with, how long it will be kept for, etc.

Question 7

Question Type: MultipleChoice

Value sensitive design focuses on which of the following?

Options:

A- Quality and benefit.

B- Ethics and morality.

C- Confidentiality and integrity.

D- Consent and human rights.

Answer:

B

Explanation:

Value sensitive design (VSD) is a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner1.It brings human values to the forefront of the technical design process2.

Question 8

Question Type: MultipleChoice

Which of the following would be an example of an "objective" privacy harm to an individual?

Options:

A- Receiving spam following the sale an of email address.

B- Negative feelings derived from government surveillance.

C- Social media profile views indicating unexpected interest in a person.

D- Inaccuracies in personal data.

Answer:

D

Explanation:

Inaccuracies in personal data would be an example of an "objective" privacy harm to an individual. This is because inaccuracies in personal data can lead to incorrect decisions being made about an individual, which can have negative consequences for the individual.

Question 9

Question Type: MultipleChoice

Which of the following occurs when an individual takes a specific observable action to indicate and confirm that they give permission for their information to be processed?

Options:

A- Express consent.

B- Implied consent.

C- Informed notice.

D- Authorized notice.

Answer:

A

Explanation:

Express consent occurs when an individual takes a specific observable action to indicate and confirm that they give permission for their information to be processed.

https://niccs.cisa.gov/education-training/catalog/international-association-privacy-professionals-iapp/certified-1

Question 10

Question Type: MultipleChoice

Which of the following is NOT a step in the methodology of a privacy risk framework?

Options:

A- Assessment.

B- Monitoring.

C- Response.

D- Ranking.

Answer:

B

Explanation:

The steps in the methodology of a privacy risk framework are Assessment, Response, and Ranking. Monitoring is not a step in the methodology of a privacy risk framework.

Question 11

Question Type: MultipleChoice

What is the most effective first step to take to operationalize Privacy by Design principles in new product development and projects?

Options:

A- Implementing a mandatory privacy review and legal approval process.

B- Obtain leadership buy-in for a mandatory privacy review and approval process.

C- Set up an online Privacy Impact Assessment tool to facilitate Privacy by Design compliance.

D- Conduct annual Privacy by Design training and refreshers for all impacted personnel.

Answer:

B

Explanation:

This is the most effective first step to operationalize Privacy by Design principles in new product development and projects. It is important to obtain leadership buy-in for a mandatory privacy review and approval process to ensure that privacy is a priority throughout the organization.