Free Questions for CDPSE by dumpshq

Shared by Bowman on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Which of the following has the GREATEST impact on the treatment of data within the scope of an organization's privacy policy?

Options:

A- Data protection impact assessment (DPIA)

B- Data flow diagram

C- Data classification

D- Data processing agreement

Answer:

C

Explanation:

Data classification is the process of categorizing data according to its sensitivity, value, and criticality for the organization and the data subjects. Data classification has the greatest impact on the treatment of data within the scope of an organization's privacy policy, as it

determines the appropriate level of protection, access, retention, and disposal for each type of dat

a. Data classification also helps to comply with the privacy principles and regulations, such as data minimization, purpose limitation, accuracy, security, and accountability.

Question 2

Which of the following MOST significantly impacts an organization's ability to respond to data subject access requests?

Options:

A- The organization's data retention schedule is complex.

B- Logging of systems and application data is limited.

C- Third-party service level agreement (SLA) data is not always available.

D- Availability of application data flow diagrams is limited.

Answer:

D

Explanation:

The availability of application data flow diagrams is the most significant factor that impacts an organization's ability to respond to data subject access requests. Data subject access requests are requests made by data subjects to exercise their rights under privacy laws or regulations, such as the right to access, rectify, erase, or port their personal data. To respond to these requests effectively and efficiently, the organization needs to have a clear and accurate understanding of how personal data is collected, processed, stored, shared, and disposed of within its applications and systems. Application data flow diagrams are graphical representations of the data lifecycle that show the sources, destinations, transformations, and dependencies of the data. Having these diagrams readily available helps the organization to locate, retrieve, modify, or delete the personal data in response to the data subject access requests. The other options are less significant or relevant than the availability of application data flow diagrams, as they do not directly affect the organization's ability to identify and access the personal data.

Question 3

Question Type: MultipleChoice

A privacy risk assessment identified that a third-party collects personal data on the organization's behalf. This finding could subject the organization to a regulatory fine for not disclosing this relationship. What should the organization do NEXT?

Options:

A- Amend the privacy policy to include a provision that data might be collected by trusted third parties.

B- Review the third-party relationship to determine who should be collecting data.

C- Update the risk assessment process to cover only required disclosures.

D- Disclose the relationship to those affected in jurisdictions where such disclosures are required.

Answer:

D

Explanation:

The organization should disclose the relationship to those affected in jurisdictions where such disclosures are required, as this is the most appropriate and compliant action to take after identifying a privacy risk related to third-party data collection. Disclosing the relationship to the data subjects is a way of providing transparency and accountability, as well as respecting their rights and choices regarding their personal data. It also helps the organization avoid regulatory fines or sanctions for not complying with the applicable privacy laws or regulations that mandate such disclosures. The other options are not as effective or sufficient as disclosing the relationship, as they do not address the root cause of the risk, do not mitigate the potential harm to the data subjects, or do not align with the privacy principles and best practices.

Question 4

Which of the following is the BEST way to ensure an organization's enterprise risk management (ERM) framework can protect the organization from privacy harms?

Options:

A- Include privacy risks as a risk category.

B- Establish a privacy incident response plan.

C- Conduct an internal privacy audit.

D- Complete a privacy risk assessment.

Answer:

D

Explanation:

The best way to ensure an organization's enterprise risk management (ERM) framework can protect the organization from privacy harms is to complete a privacy risk assessment. A privacy risk assessment is a systematic process of identifying, analyzing, evaluating, and treating the privacy risks that may affect the organization's objectives, operations, stakeholders, and reputation. A privacy risk

assessment helps to align the ERM framework with the privacy requirements, expectations, and obligations of the organization, as well as to prioritize and mitigate the privacy risks that may cause privacy harms. Privacy harms are the adverse consequences or impacts that may result from the unauthorized or inappropriate use, disclosure, or loss of personal data, such as financial loss, identity theft, discrimination, reputational damage, emotional distress, or physical harm.

Question 5

Critical data elements should be mapped to which of the following?

Options:

A- Data process flow

B- Business analytics

C- Business taxonomy

D- Privacy policy

Answer:

A

Critical data elements are the data elements that are essential for the organization to achieve its business objectives, comply with legal and regulatory requirements, and protect the privacy and security of the data subjects. Critical data elements should be mapped to the data process flow, which is a graphical representation of how data is collected, processed, stored, shared, and disposed of within the organization. Mapping critical data elements to the data process flow helps to identify the sources, destinations, transformations, and dependencies of the data, as well as the potential risks and controls associated with each step of the data lifecycle.

Question 6

Question Type: MultipleChoice

Which of the following is the BEST control to prevent the exposure of personal information when redeploying laptops within an organization?

Options:

A- Set a unique static IP for the default network interface.

B- Disable all wireless networking in the group policy.

C- Reinstall the operating system and enable laptop encryption.

D- Perform a full wipe and reimage of the laptops.

Answer:

D

Explanation:

Performing a full wipe and reimage of the laptops is the best control to prevent the exposure of personal information when redeploying laptops within an organization. This is because a full wipe and reimage ensures that all data, including personal information, is securely erased from the laptops and replaced with a fresh installation of the operating system and applications. This reduces the risk of data leakage, unauthorized access, or data recovery by malicious actors or unauthorized users. The other options are not as effective or sufficient as a full wipe and reimage, as they do not guarantee the complete removal of personal information from the laptops.

Question 7

Question Type: MultipleChoice

Which of the following outputs of a privacy audit is MOST likely to trigger remedial action?

Options:

A- Deficiencies in how personal data is shared with third parties

B- Recommendations to optimize current privacy policy

C- Identification of uses of sensitive personal data

D- Areas of focus for privacy training

Answer:

A

Explanation:

A privacy audit is a systematic and independent examination of an organization's privacy policies, procedures, practices, and controls to assess their compliance with applicable laws, regulations, standards, and best practices. A privacy audit may result in various outputs, such as findings, recommendations, observations, or opinions. Among the options given, the output that is most likely to trigger remedial action is the identification of deficiencies in how personal data is shared with third parties. This is because such deficiencies may pose significant risks to the privacy and security of the data subjects, as well as to the reputation and legal liability of the organization. Remedial action may include implementing contractual safeguards, technical measures, or organizational changes to ensure that third parties respect and protect the personal data they receive from the organization.