Free Questions for CDPSE

Shared by Peck on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following information would MOST likely be considered sensitive personal data?

Options:

A- Mailing address
B- Bank account login ID
C- Ethnic origin
D- Contact phone number

Answer:

C

Explanation:

Sensitive personal data is a subset of personal data that reveals or relates to more intimate or confidential aspects of a person's identity, such as their racial or ethnic origin, religious or philosophical beliefs, health status, sexual orientation, political opinions, trade union membership, biometric or genetic data, or criminal record. Sensitive personal data is subject to more stringent legal and regulatory protections and requires a higher level of consent from the data subject to be processed. Mailing address, bank account login ID, and contact phone number are examples of personal data, but not sensitive personal data, as they do not reveal or relate to such intimate or confidential aspects of a person's identity.

Question 2

Question Type: MultipleChoice

A migration of personal data involving a data source with outdated documentation has been approved by senior management. Which of the following should be done NEXT?

Options:

A- Review data flow post migration.
B- Ensure appropriate data classification.

C- Engage an external auditor to review the source data.
D- Check the documentation version history for anomalies.

Answer:

B

Explanation:

Ensuring appropriate data classification should be done next after a migration of personal data involving a data source with outdated documentation has been approved by senior management, as it helps to identify the types, locations, and owners of the data, and to apply the appropriate privacy controls and measures based on the data classification level.Data classification also facilitates the data discovery, data minimization, data retention, and data disposal processes15.Reference:1Domain 3, Task 2;5Page 9

Question 3

Question Type: MultipleChoice

Which of the following is the MOST important privacy consideration when developing a contact tracing application?

Options:

A- The proportionality of the data collected tor the intended purpose
B- Whether the application can be audited for compliance purposes
C- The creation of a clear privacy notice
D- Retention period for data storage

Answer:

A

Explanation:

The proportionality of the data collected for the intended purpose is the most important privacy consideration when developing a contact tracing application.This means that the application should only collect the minimum amount of personal data necessary to achieve the specific and legitimate purpose of preventing and controlling the spread of COVID-191.The application should

also ensure that the data collected are relevant, adequate, and not excessive in relation to the purpose2.The application should avoid collecting or processing any data that are not essential for the purpose, such as location data, biometric data, or health data unrelated to COVID-193.The application should also respect the data minimization principle, which requires that the data are kept for no longer than necessary for the purpose4.Reference:

European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak

Article 5(1) of the General Data Protection Regulation (GDPR)

Article 29 Data Protection Working Party Opinion 04/2017 on the Proposed Regulation for the ePrivacy Regulation

Article 5(1)(e) of the GDPR

Question 4

Question Type: MultipleChoice

Which of the following is a responsibility of the audit function in helping an organization address privacy compliance requirements?

Options:

A- Approving privacy impact assessments (PIAs)
B- Validating the privacy framework
C- Managing privacy notices provided to customers
D- Establishing employee privacy rights and consent

Answer:

B

Explanation:

Validating the privacy framework is a responsibility of the audit function in helping an organization address privacy compliance requirements, as it would help to verify and validate the effectiveness and adequacy of the privacy framework implemented by the organization to comply with privacy principles, laws and regulations. Validating the privacy framework would also help to identify and report any gaps, weaknesses or issues in the privacy framework, and to provide recommendations for improvement or remediation. The other options are not responsibilities of

the audit function in helping an organization address privacy compliance requirements. Approving privacy impact assessments (PIAs) is a responsibility of management or governance function in helping an organization address privacy compliance requirements, as they would have authority and accountability for approving PIAs conducted by project teams or business units before implementing any system, project, program or initiative that involves personal data processing activities. Managing privacy notices provided to customers is a responsibility of operational function in helping an organization address privacy compliance requirements, as they would have direct contact and interaction with customers and would be responsible for providing clear and accurate information about how their personal data is collected, used, disclosed and transferred by the organization.

Question 5

Question Type: MultipleChoice

A health organization experienced a breach of a database containing pseudonymized personal dat

a. Which of the following should be of MOST concern to the IT privacy practitioner?

Options:

A- The data may be re-identified.
B- The data was proprietary.
C- The data was classified as confidential.
D- The data is subject to regulatory fines.

Answer:

A

Explanation:

Pseudonymization is a technique that replaces or removes direct identifiers from personal data, such as names, addresses, or social security numbers, with pseudonyms, such as codes, tokens, or random values. However, pseudonymization does not eliminate the possibility of re-identification, as the original data can still be linked back to the pseudonyms using additional information or techniques. Therefore, if a database containing pseudonymized personal data is breached, the IT privacy practitioner should be most concerned about the risk of re-identification, which could compromise the privacy and security of the data subjects. The other options are less relevant or important than the risk of re-identification.

Question 6

Question Type: MultipleChoice

Which of the following is MOST important when designing application programming interfaces (APIs) that enable mobile device applications to access personal data?

Options:

A- The user's ability to select, filter, and transform data before it is shared
B- Umbrella consent for multiple applications by the same developer
C- User consent to share personal data
D- Unlimited retention of personal data by third parties

Answer:

C

Explanation:

User consent to share personal data is the most important factor when designing APIs that enable mobile device applications to access personal data, as it ensures that the user is informed and agrees to the purpose, scope, and duration of the data sharing.User consent also helps to comply with the data protection principles and regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), that require user consent for certain types of data processing and sharing134.Reference:1Domain 2, Task 7

Question 7

Question Type: MultipleChoice

Which of the following is the MOST important consideration for determining the operational life of an encryption key?

Options:

A- Number of entities involved in communication
B- Number of digitally signed documents in force

C- Volume and sensitivity of data protected
D- Length of key and complexity of algorithm

Answer:

C

Explanation:

The most important consideration for determining the operational life of an encryption key is the volume and sensitivity of data protected by the key. The operational life of an encryption key is the period of time during which the key can be used securely and effectively to encrypt and decrypt data. The operational life of an encryption key depends on various factors, such as the length and complexity of the key, the strength and speed of the encryption algorithm, the number and frequency of encryption operations, the number of entities involved in communication, and the number of digitally signed documents in force. However, among these factors, the volume and sensitivity of data protected by the key is the most critical, as it affects the risk and impact of a potential compromise or exposure of the key. The higher the volume and sensitivity of data protected by the key, the shorter the operational life of the key should be, as this reduces the window of opportunity for an attacker to access or misuse the data.

Question 8

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.

Question 9

Question Type: MultipleChoice

Which of the following BEST mitigates the privacy risk associated with setting cookies on a website?

Options:

A- Implementing impersonation
B- Obtaining user consent
C- Ensuring nonrepudiation
D- Applying data masking

Answer:

B

Explanation:

Obtaining user consent is the best way to mitigate the privacy risk associated with setting cookies on a website. This means that the website should inform the users about the purpose, type, and duration of the cookies, and ask for their permission before storing or accessing any cookies on their browsers. This way, the users can exercise their right to control their personal data and opt-in or opt-out of cookies as they wish.

According to the General Data Protection Regulation (GDPR), consent must be freely given, specific, informed, and unambiguous. The website should provide clear and easy-to-understand information about the cookies and their implications for the users' privacy, and offer a simple and effective way for the users to indicate their consent or refusal. The website should also respect

the users' choice and allow them to withdraw their consent at any time.

Implementing impersonation, ensuring nonrepudiation, and applying data masking are not relevant or effective methods to mitigate the privacy risk associated with setting cookies on a website. Impersonation means accessing or using data on behalf of another user, which could violate their privacy and security. Nonrepudiation means providing proof of the origin, authenticity, and integrity of data, which does not address the issue of user consent or preference. Data masking means hiding or replacing sensitive data with fake or modified data, which does not prevent the storage or access of cookies on the user's browser.

Question 10

Question Type: MultipleChoice

An online business posts its customer data protection notice that includes a statement indicating information is collected on how products are used, the content viewed, and the time and duration of online activities. Which data protection principle is applied?

Options:

A- System use requirements
B- Data integrity and confidentiality
C- Lawfulness and fairness
D- Data use limitation

Answer:

C

Explanation:

The data protection principle that is applied when an online business posts its customer data protection notice that includes a statement indicating information is collected on how products are used, the content viewed, and the time and duration of online activities is lawfulness and fairness. Lawfulness and fairness are two of the core principles of data protection under various laws and regulations, such as the GDPR or the CCPA. They state that personal data should be processed lawfully, fairly and in a transparent manner in relation to the data subject. By posting a customer data protection notice that informs customers about what information is collected and for what purpose, the online business demonstrates its compliance with these principles.

System use requirements, data integrity and confidentiality, or data use limitation are not the

correct names of the data protection principles that are applied in this case. System use requirements are not a specific principle of data protection, but rather a general term that refers to the rules or policies that govern how users can access and use a system or service. Data integrity and confidentiality are two aspects of the security principle of data protection, which states that personal data should be processed in a manner that ensures appropriate security of the personal data. Data use limitation is not a specific principle of data protection either, but rather a concept that relates to the purpose limitation principle, which states that personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.