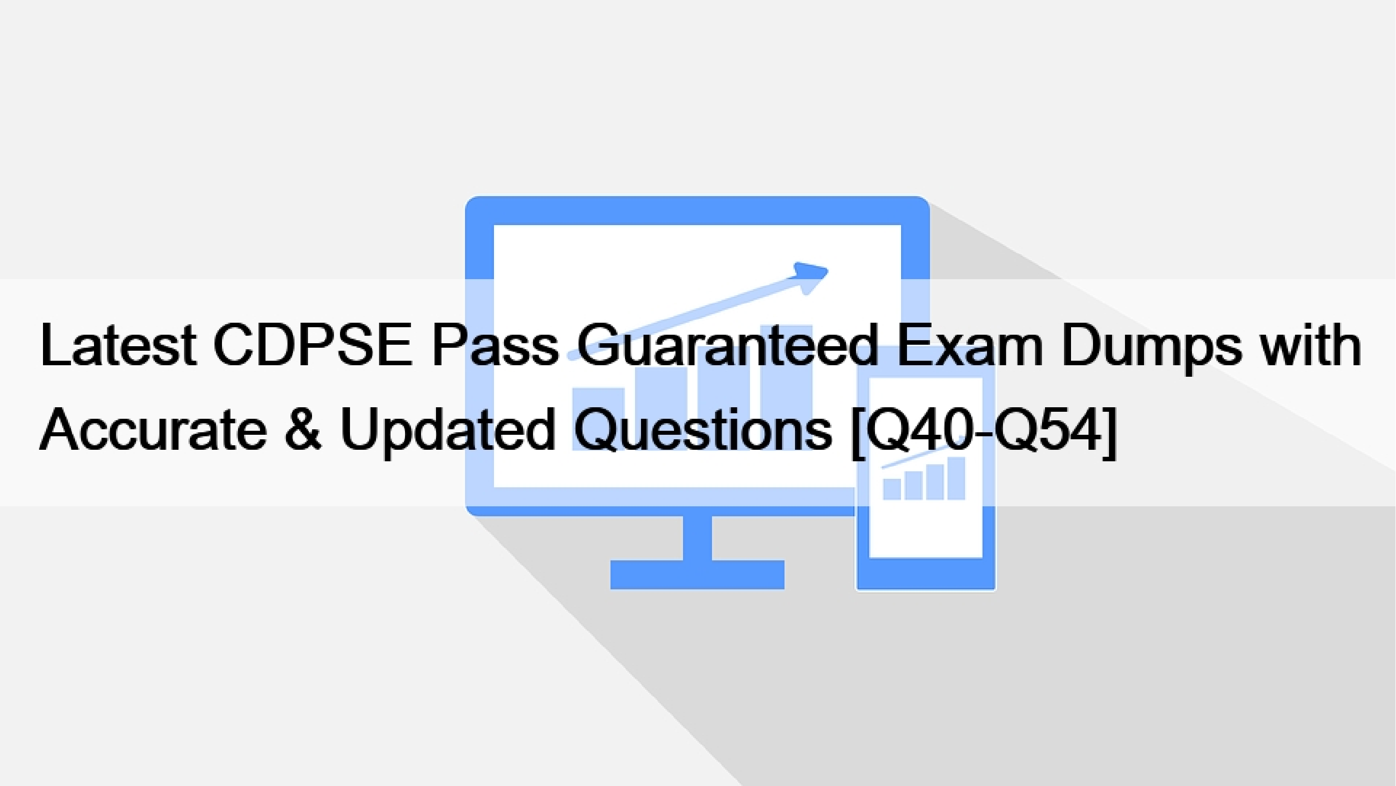
Latest CDPSE Pass Guaranteed Exam Dumps with Accurate & Updated Questions [Q40-Q54


Latest CDPSE Pass Guaranteed Exam Dumps with Accurate & Updated Questions [Q40-Q54]

Latest CDPSE Pass Guaranteed Exam Dumps with Accurate & Updated Questions
CDPSE Exam Brain Dumps - Study Notes and Theory

The CDPSE certification is designed to help professionals demonstrate their knowledge and skills in various areas, including data privacy and protection, risk management, compliance, governance, and data security. Certified Data Privacy Solutions Engineer certification exam covers a range of topics, including privacy regulations, data protection laws, privacy program management, privacy by design, data security, and risk management. Certified Data Privacy Solutions Engineer certification is ideal for professionals who want to demonstrate their expertise in data privacy and security and advance their careers in this field.

Q40. Which of the following is the MOST important action to protect a mobile banking app and its data against manipulation and disclosure?
* Define the mobile app privacy policy.
* Implement application hardening measures.
* Provide the app only through official app stores
* Conduct penetration testing
Explanation

Application hardening measures are the most important action to protect a mobile banking app and its data against manipulation and disclosure because they prevent attackers from reverse engineering, tampering, or injecting malicious code into the app. Application hardening measures include techniques such as code obfuscation, encryption, integrity checks, anti-debugging, and anti-tampering mechanisms. These measures make the app more resilient and secure against various types of cyberattacks.

References:

* ISACA Certified Data Privacy Solutions Engineer Study Guide, Domain 3: Privacy Engineering, Task

3.4: Implement privacy engineering techniques to protect data in applications and systems, p. 104-105.

* What is Application Hardening? | Glossary | Digital.ai

Q41. When using pseudonymization to prevent unauthorized access to personal data, which of the following is the MOST important consideration to ensure the data is adequately protected?
* The data must be protected by multi-factor authentication.
* The identifier must be kept separate and distinct from the data it protects.
* The key must be a combination of alpha and numeric characters.
* The data must be stored in locations protected by data loss prevention (DLP) technology.

Q42. Which of the following is the BEST way to address privacy concerns when an organization captures personal data from a third party through an open application programming interface (API)?
* Develop a service level agreement (SLA) with the third party
* Implement encryption for the data transmission
* Obtain consent from the data subjects
* Review the specification document of the open API.

Explanation

The best way to address privacy concerns when an organization captures personal data from a third party through an open application programming interface (API) is to obtain consent from the data subjects. Consent is a freely given, specific, informed, and unambiguous indication of the data subject&#8217;s wishes by which they agree to the processing of their personal data by the organization for a defined purpose. Consent is one of the legal bases for processing personal data under various privacy laws and regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). Obtaining consent from the data subjects can help ensure that they are aware of and agree to the collection and use of their personal data by the organization through the open API. Obtaining consent can also help respect the data subject&#8217;s rights and preferences regarding their personal data.

Developing a service level agreement (SLA) with the third party, implementing encryption for the data transmission, or reviewing the specification document of the open API are also good practices for addressing privacy concerns when using an open API to capture personal data from a third party, but they are not the best way. Developing an SLA with the third party can help define the roles, responsibilities, expectations, and obligations of both parties regarding the provision and use of the open API and the personal data involved.

Implementing encryption for the data transmission can help protect the confidentiality, integrity, and availability of the personal data transferred between the third party and the organization through the open API.

Reviewing the specification document of the open API can help understand the functionality, features, parameters, or requirements of the open API and how it handles personal data.

References: Open APIs and Security Risks | Govenda Board Portal Software, The top API security risks and how to mitigate them &#8211; Appinventiv, Critical API security risks: 10 best practices | TechBeacon

Q43. Which of the following should be the FIRST consideration when conducting a privacy impact assessment (PIA)?
* The applicable privacy legislation
* The quantity of information within the scope of the assessment
* The systems in which privacy-related data is stored
* The organizational security risk profile
Explanation

The first consideration when conducting a privacy impact assessment (PIA) is the applicable privacy legislation that governs the collection, processing, storage, transfer, and disposal of personal data within the scope of the assessment. The applicable privacy legislation may vary depending on the jurisdiction, sector, or purpose of the data processing activity. The PIA should identify and comply with the relevant legal requirements and obligations for data protection and privacy, such as obtaining consent, providing notice, ensuring data quality and security, respecting data subject rights, and reporting data breaches. The applicable privacy legislation also determines the criteria, methodology, and documentation for conducting the PIA.

References:

* ISACA, Performing an Information Security and Privacy Risk Assessment1

* ISACA, Best Practices for Privacy Audits2

* ISACA, GDPR Data Protection Impact Assessments3

* ISACA, GDPR Data Protection Impact Assessment Template4

Q44. Which of the following rights is an important consideration that allows data subjects to request the deletion of their data?
* The right to object
* The right to withdraw consent
* The right to access
* The right to be forgotten

Q45. Which of the following is the GREATEST benefit of adopting data minimization practices?
* Storage and encryption costs are reduced.
* Data retention efficiency is enhanced.
* The associated threat surface is reduced.
* Compliance requirements are met.
Unfortunately, the financial liability portion of retained personal information rarely shows up on an organization&#8217;s financial balance sheet. And yet it is indeed a liability: the impact on an organization when cybercriminals steal that information or when the information is misused is real, in the form of breach response costs, the costs related to reducing harm inflicted on affected parties (think of credit monitoring services, a frequent remedy for stolen credit card numbers), fines from governmental regulators, and the occasional class-action lawsuit.

Q46. Which of the following is the BEST indication of an effective records management program for personal data?
* Archived data is used for future analytics.
* The legal department has approved the retention policy.
* All sensitive data has been tagged.
* A retention schedule is in place.
Explanation

A retention schedule is a document that specifies how long different types of records or data should be kept and when they should be deleted or disposed of, based on legal, regulatory, operational or historical requirements. A retention schedule is the best indication of an effective records management program for personal data, as it reflects the principles of data minimization and storage limitation, which require limiting the collection, storage and processing of personal data to what is necessary and relevant for the intended purposes, and deleting or disposing of personal data when it is no longer needed or justified. A retention schedule also helps to reduce the privacy risks and costs associated with data storage and retention, such as data breaches, unauthorized access, misuse or loss of data. The other options are not as indicative of an effective records management program for personal data as a retention schedule. Archived data is used for future analytics may indicate that the organization is leveraging its data assets for business intelligence or research purposes, but it may not comply with the principles of data minimization and storage limitation, or the privacy rights and preferences of the data subjects. The legal department has approved the retention policy may indicate that the organization has obtained legal advice or guidance on its records management program for personal data, but it may not reflect the actual implementation or execution of the retention policy. All sensitive data has been tagged may indicate that the organization has implemented a data classification scheme for its records or data, but it may not indicate how long the records or data should be kept or when they should be deleted or disposed of1, p. 99-100 References: 1: CDPSE Review Manual (Digital Version)

Q47. Data collected by a third-party vendor and provided back to the organization may not be protected according to the organization&#8217;s privacy notice. Which of the following is the BEST way to address this concern?
* Review the privacy policy.
* Obtain independent assurance of current practices.
* Re-assess the information security requirements.
* Validate contract compliance.

Q48. Which of the following is a responsibility of the audit function in helping an organization address privacy compliance requirements?
* Approving privacy impact assessments (PIAs)
* Validating the privacy framework
* Managing privacy notices provided to customers
* Establishing employee privacy rights and consent

Q49. Which of the following would MOST effectively reduce the impact of a successful breach through a remote access solution?
* Compartmentalizing resource access
* Regular testing of system backups
* Monitoring and reviewing remote access logs
* Regular physical and remote testing of the incident response plan

Q50. A new marketing application needs to use data from the organization&#8217;s customer database. Prior to the application using the data, which of the following should be done FIRST?
* Ensure the data loss prevention (DLP) tool is logging activity.
* De-identify all personal data in the database.
* Determine what data is required by the application.
* Renew the encryption key to include the application.
Explanation

Before using data from the organization&#8217;s customer database for a new marketing application, the first step should be to determine what data is required by the application and for what purpose. This will help to ensure that the data collection and processing are relevant, necessary, and proportionate to the intended use, and that the data minimization principle is followed. Data minimization means that only the minimum amount of personal data needed to achieve a specific purpose should be collected and processed, and that any excess or irrelevant data should be deleted or anonymized1. This will also help to comply with the data privacy laws and regulations that apply to the organization, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), which require organizations to inform data subjects about the types and purposes of data processing, and to obtain their consent if needed23.

References:

* ISACA, Data Privacy Audit/Assurance Program, Control Objective 2: Data Minimization, p. 61

* ISACA, GDPR Data Protection Impact Assessments, p. 4-52

* ISACA, CCPA vs. GDPR: Similarities and Differences, p. 1-23

Q51. What is the PRIMARY means by which an organization communicates customer rights as it relates to the use of their personal information?
* Distributing a privacy rights policy
* Mailing rights documentation to customers
* Publishing a privacy notice
* Gaining consent when information is collected
Explanation

The primary means by which an organization communicates customer rights as it relates to the use of their personal information is publishing a privacy notice. A privacy notice is a document that informs the customers about how their personal information is collected, used, shared, stored, and protected by the organization, as well as what rights they have regarding their personal information, such as access, rectification, erasure, portability, objection, etc. A privacy notice should be clear, concise, transparent, and easily accessible to the customers, and should comply with the applicable privacy regulations and standards. A privacy notice helps to establish trust and transparency between the organization and the customers, and enables the customers to exercise their rights and choices over their personal information. References: : CDPSE Review Manual (Digital Version), page 39

Q52. Which of the following vulnerabilities would have the GREATEST impact on the privacy of information?
* Private key exposure
* Poor patch management
* Lack of password complexity
* Out-of-date antivirus signatures
Explanation

The vulnerability that would have the greatest impact on the privacy of information is private key exposure, because it would compromise the encryption and decryption of the information, as well as the authentication and integrity of the communicating parties. A private key is a secret and unique value that is used to encrypt or decrypt data, or to sign or verify digital signatures. If an attacker gains access to the private key, they can read, modify, or impersonate the data or the sender, which would violate the confidentiality, integrity, and authenticity of the information12.

References:

* CDPSE Review Manual, Chapter 2 &#8211; Privacy Architecture, Section 2.3 &#8211; Privacy Architecture Implementation3.

* CDPSE Certified Data Privacy Solutions Engineer All-in-One Exam Guide, Chapter 2 &#8211; Privacy

* Architecture, Section 2.4 &#8211; Remote Access4.

Q53. An organization is creating a personal data processing register to document actions taken with personal dat a. Which of the following categories should document controls relating to periods of retention for personal data?
* Data archiving
* Data storage
* Data acquisition

* Data input
However, the risks associated with long-term retention have compelled organizations to consider alternatives; one is data archival, the process of preparing data for long-term storage. When organizations are bound by specific laws to retain data for many years, archival provides a viable opportunity to remove data from online transaction systems to other systems or media.

Q54. Which type of data is produced by using a more complex method of analytics to find correlations between data sets and using them to categorize or profile people?
* Observed data
* Inferred data
* Derived data
* Provided data
Explanation

Inferred data is the type of data that is produced by using a more complex method of analytics to find correlations between data sets and using them to categorize or profile people. Inferred data is not directly observed or collected from the data subjects, but rather derived from other sources of data, such as behavioral, transactional, or demographic data. Inferred data can be used to make assumptions or predictions about the data subjects&#8217; preferences, interests, behaviors, or characteristics12.

References:

* CDPSE Review Manual, Chapter 3 &#8211; Data Lifecycle, Section 3.1 &#8211; Data Classification3.

* CDPSE Certified Data Privacy Solutions Engineer All-in-One Exam Guide, Chapter 3 &#8211; Data Lifecycle, Section 3.2 &#8211; Data Classification4.

ISACA CDPSE (Certified Data Privacy Solutions Engineer) certification exam is a globally recognized credential that validates an individual's expertise in data privacy solutions engineering. CDPSE exam is designed for IT professionals who are responsible for developing, implementing, and managing data privacy solutions in an organization. Certified Data Privacy Solutions Engineer certification demonstrates an individual's ability to assess and manage privacy risks, design and implement data privacy solutions, and ensure compliance with privacy regulations.

Pass ISACA CDPSE Test Practice Test Questions Exam Dumps:
https://www.examcollectionpass.com/ISACA/CDPSE-practice-exam-dumps.html]