Exam Questions CDPSE

Certified Data Privacy Solutions Engineer

https://www.2passeasy.com/dumps/CDPSE/

NEW QUESTION 1
When choosing data sources to be used within a big data architecture, which of the following data attributes MUST be considered to ensure data is not aggregated?

A. Accuracy
B. Granularity
C. Consistency
D. Reliability

Answer: B

NEW QUESTION 2
Which of the following should be used to address data kept beyond its intended lifespan?

A. Data minimization
B. Data anonymization
C. Data security
D. Data normalization

Answer: A

NEW QUESTION 3
Which of the following techniques mitigates design flaws in the application development process that may contribute to potential leakage of personal data?

A. User acceptance testing (UAT)
B. Patch management
C. Software hardening
D. Web application firewall (WAF)

Answer: A

NEW QUESTION 4
Which of the following is the MOST important consideration when using advanced data sanitization methods to ensure privacy data will be unrecoverable?

A. Subject matter expertise
B. Type of media
C. Regulatory compliance requirements
D. Location of data

Answer: C

NEW QUESTION 5
When evaluating cloud-based services for backup, which of the following is MOST important to consider from a privacy regulation standpoint?

A. Data classification labeling
B. Data residing in another country
C. Volume of data stored
D. Privacy training for backup users

Answer: A

NEW QUESTION 6
Which of the following is the GREATEST benefit of adopting data minimization practices?

A. Storage and encryption costs are reduced.
B. Data retention efficiency is enhanced.
C. The associated threat surface is reduced.
D. Compliance requirements are met.

Answer: B

Explanation:
Unfortunately, the financial liability portion of retained personal information rarely shows up on an organization’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.

NEW QUESTION 7
Which of the following is MOST important when developing an organizational data privacy program?

A. Obtaining approval from process owners
B. Profiling current data use
C. Following an established privacy framework
D. Performing an inventory of all data

Answer: D

NEW QUESTION 8
Which of the following zones within a data lake requires sensitive data to be encrypted or tokenized?

A. Trusted zone
B. Clean zone
C. Raw zone
D. Temporal zone

Answer: D

NEW QUESTION 9
An organization is planning a new implementation for tracking consumer web browser activity. Which of the following should be done FIRST?

A. Seek approval from regulatory authorities.
B. Conduct a privacy impact assessment (PIA).
C. Obtain consent from the organization's clients.
D. Review and update the cookie policy.

Answer: A

NEW QUESTION 10
Which of the following is a PRIMARY objective of performing a privacy impact assessment (PIA) prior to onboarding a new Software as a Service (SaaS) provider for a customer relationship management (CRM) system?

A. To identify controls to mitigate data privacy risks
B. To classify personal data according to the data classification scheme
C. To assess the risk associated with personal data usage
D. To determine the service provider's ability to maintain data protection controls

Answer: D

NEW QUESTION 10
Which of the following should be the FIRST consideration when conducting a privacy impact assessment (PIA)?

A. The applicable privacy legislation
B. The quantity of information within the scope of the assessment
C. The systems in which privacy-related data is stored
D. The organizational security risk profile

Answer: C

NEW QUESTION 15
Which of the following vulnerabilities is MOST effectively mitigated by enforcing multi-factor authentication to obtain access to personal information?

A. End users using weak passwords
B. Organizations using weak encryption to transmit data
C. Vulnerabilities existing in authentication pages
D. End users forgetting their passwords

Answer: A

NEW QUESTION 18
Which of the following BEST enables an IT privacy practitioner to ensure appropriate protection for personal data collected that is required to provide necessary services?

A. Understanding the data flows within the organization
B. Implementing strong access controls on a need-to-know basis
C. Anonymizing privacy data during collection and recording
D. Encrypting the data throughout its life cycle

Answer: A

NEW QUESTION 22
Which of the following is the PRIMARY reason to complete a privacy impact assessment (PIA)?

A. To comply with consumer regulatory requirements
B. To establish privacy breach response procedures
C. To classify personal data
D. To understand privacy risks

Answer: A

NEW QUESTION 24
Which key stakeholder within an organization should be responsible for approving the outcomes of a privacy impact assessment (PIA)?

A. Data custodian
B. Privacy data analyst
C. Data processor
D. Data owner

Answer: D

NEW QUESTION 26
Which authentication practice is being used when an organization requires a photo on a government-issued identification card to validate an in-person credit card purchase?

A. Possession factor authentication
B. Knowledge-based credential authentication
C. Multi-factor authentication
D. Biometric authentication

Answer: B

NEW QUESTION 30
Which of the following is the BEST approach to minimize privacy risk when collecting personal data?

A. Use a third party to collect, store, and process the data.
B. Collect data through a secure organizational web server.
C. Collect only the data necessary to meet objectives.
D. Aggregate the data immediately upon collection.

Answer: C

NEW QUESTION 35
Which of the following is a responsibility of the audit function in helping an organization address privacy compliance requirements?

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: D

NEW QUESTION 36
Which of the following is MOST likely to present a valid use case for keeping a customer's personal data after contract termination?

A. For the purpose of medical research
B. A forthcoming campaign to win back customers
C. A required retention period due to regulations
D. Ease of onboarding when the customer returns

Answer: C

NEW QUESTION 38
What is the BEST way for an organization to maintain the effectiveness of its privacy breach incident response plan?

A. Require security management to validate data privacy security practices.
B. Involve the privacy office in an organizational review of the incident response plan.
C. Hire a third party to perform a review of data privacy processes.
D. Conduct annual data privacy tabletop exercises.

Answer: A

Explanation:
Because many privacy incidents are also security incidents, the development of a privacy incident response plan should be performed in close cooperation with the security manager to avoid duplication of effort and to utilize existing response plan resources and practices.

NEW QUESTION 42
Which party should data subject contact FIRST if they believe their personal information has been collected and used without consent?

A. Privacy rights advocate
B. Outside privacy counsel
C. Data protection authorities
D. The organization's chief privacy officer (CPO)

Answer: C

NEW QUESTION 46
Which of the following is the BEST way for an organization to limit potential data exposure when implementing a new application?

A. Implement a data loss prevention (DLP) system.
B. Use only the data required by the application.
C. Encrypt all data used by the application.
D. Capture the application's authentication logs.

Answer: A

NEW QUESTION 50
An email opt-in form on a website applies to which privacy principle?

A. Accuracy
B. Consent
C. Transparency
D. Integrity

Answer: B

NEW QUESTION 55
Which of the following is the BEST approach for a local office of a global organization faced with multiple privacy-related compliance requirements?

A. Focus on developing a risk action plan based on audit reports.
B. Focus on requirements with the highest organizational impact.
C. Focus on global compliance before meeting local requirements.
D. Focus on local standards before meeting global compliance.

Answer: D

NEW QUESTION 57
Data collected by a third-party vendor and provided back to the organization may not be protected according to the organization's privacy notice. Which of the following is the BEST way to address this concern?

A. Review the privacy policy.
B. Obtain independent assurance of current practices.
C. Re-assess the information security requirements.
D. Validate contract compliance.

Answer: C

NEW QUESTION 60
Before executive leadership approves a new data privacy policy, it is MOST important to ensure:

A. a training program is developed.
B. a privacy committee is established.
C. a distribution methodology is identified.
D. a legal review is conducted.

Answer: B

NEW QUESTION 64
What is the BEST method to protect customers' personal data that is forwarded to a central system for analysis?

A. Pseudonymization
B. Deletion
C. Encryption
D. Anonymization

Answer: C

NEW QUESTION 68
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?

A. The data must be protected by multi-factor authentication.
B. The identifier must be kept separate and distinct from the data it protects.
C. The key must be a combination of alpha and numeric characters.
D. The data must be stored in locations protected by data loss prevention (DLP) technology.

Answer: D

NEW QUESTION 70
Which of the following tracking technologies associated with unsolicited targeted advertisements presents the GREATEST privacy risk?

A. Online behavioral tracking
B. Radio frequency identification (RFID)
C. Website cookies
D. Beacon-based tracking

Answer: C

NEW QUESTION 75
Which of the following is the best reason for a health organization to use desktop virtualization to implement stronger access control to systems containing patient records?

A. Limited functions and capabilities of a secured operating environment
B. Monitored network activities for unauthorized use
C. Improved data integrity and reduced effort for privacy audits
D. Unlimited functionalities and highly secured applications

Answer: B

NEW QUESTION 80
How can an organization BEST ensure its vendors are complying with data privacy requirements defined in their contracts?

A. Review self-attestations of compliance provided by vendor management.
B. Obtain independent assessments of the vendors' data management processes.
C. Perform penetration tests of the vendors' data security.
D. Compare contract requirements against vendor deliverables.

Answer: D

NEW QUESTION 82
Of the following, who should be PRIMARILY accountable for creating an organization's privacy management strategy?

A. Chief data officer (CDO)
B. Privacy steering committee
C. Information security steering committee
D. Chief privacy officer (CPO)

Answer: D

Explanation:
Some organizations, typically those that manage large amounts of personal information related to employees, customers, or constituents, will employ a chief privacy officer (CPO). Some organizations have a CPO because applicable regulations such as the Gramm-Leach-Bliley Act (GLBA) require it. Other regulations such as the Health Information Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the GLBA place a slate of responsibilities upon an organization that compels them to hire an executive responsible for overseeing compliance.

NEW QUESTION 87
Which of the following is the BEST way to distinguish between a privacy risk and compliance risk?

A. Perform a privacy risk audit.
B. Conduct a privacy risk assessment.
C. Validate a privacy risk attestation.
D. Conduct a privacy risk remediation exercise.

Answer: A

NEW QUESTION 88
Which of the following is the BEST control to secure application programming interfaces (APIs) that may contain personal information?

A. Encrypting APIs with the organization's private key
B. Requiring nondisclosure agreements (NDAs) when sharing APIs
C. Restricting access to authorized users
D. Sharing only digitally signed APIs

Answer: C

NEW QUESTION 93
Which of the following should be done FIRST when developing an organization-wide strategy to address data privacy risk?

A. Obtain executive support.
B. Develop a data privacy policy.
C. Gather privacy requirements from legal counsel.
D. Create a comprehensive data inventory.

Answer: D

NEW QUESTION 94

Which types of controls need to be applied to ensure accuracy at all stages of processing, storage, and deletion throughout the data life cycle?

A. Processing flow controls
B. Time-based controls
C. Purpose limitation controls
D. Integrity controls

Answer: D

NEW QUESTION 99
Which of the following MUST be available to facilitate a robust data breach management response?

A. Lessons learned from prior data breach responses
B. Best practices to obfuscate data for processing and storage
C. An inventory of previously impacted individuals
D. An inventory of affected individuals and systems

Answer: A

NEW QUESTION 100
An organization is concerned with authorized individuals accessing sensitive personal customer information to use for unauthorized purposes. Which of the following technologies is the BEST choice to mitigate this risk?

A. Email filtering system
B. Intrusion monitoring
C. Mobile device management (MDM)
D. User behavior analytics

Answer: B

NEW QUESTION 104
Which of the following describes a user's "right to be forgotten"?

A. The data is being used to comply with legal obligations or the public interest.
B. The data is no longer required for the purpose originally collected.
C. The individual objects despite legitimate grounds for processing.
D. The individual's legal residence status has recently changed.

Answer: A

NEW QUESTION 105
When configuring information systems for the communication and transport of personal data, an organization should:

A. adopt the default vendor specifications.
B. review configuration settings for compliance.
C. implement the least restrictive mode.
D. enable essential capabilities only.

Answer: B

NEW QUESTION 106
A global organization is planning to implement a customer relationship management (CRM) system to be used in offices based in multiple countries. Which of the following is the MOST important data protection consideration for this project?

A. Industry best practice related to information security standards in each relevant jurisdiction
B. Identity and access management mechanisms to restrict access based on need to know
C. Encryption algorithms for securing customer personal data at rest and in transit
D. National data privacy legislative and regulatory requirements in each relevant jurisdiction

Answer: B

NEW QUESTION 111
Which of the following is the PRIMARY consideration to ensure control of remote access is aligned to the privacy policy?

A. Access is logged on the virtual private network (VPN).
B. Multi-factor authentication is enabled.
C. Active remote access is monitored.
D. Access is only granted to authorized users.

Answer: D

NEW QUESTION 113
An organization uses analytics derived from archived transaction data to create individual customer profiles for customizing product and service offerings. Which of the following is the IT privacy practitioner's BEST recommendation?

A. Anonymize personal data.
B. Discontinue the creation of profiles.
C. Implement strong access controls.
D. Encrypt data at rest.

Answer: A

NEW QUESTION 114
Which of the following protocols BEST protects end-to-end communication of personal data?

A. Transmission Control Protocol (TCP)
B. Transport Layer Security Protocol (TLS)
C. Secure File Transfer Protocol (SFTP)
D. Hypertext Transfer Protocol (HTTP)

Answer: B

NEW QUESTION 119
Which of the following BEST supports an organization's efforts to create and maintain desired privacy protection practices among employees?

A. Skills training programs
B. Awareness campaigns
C. Performance evaluations
D. Code of conduct principles

Answer: B

NEW QUESTION 122
An organization want to develop an application programming interface (API) to seamlessly exchange personal data with an application hosted by a third-party service provider. What should be the FIRST step when developing an application link?

A. Data tagging
B. Data normalization
C. Data mapping
D. Data hashing

Answer: C

NEW QUESTION 123
When a government's health division established the complete privacy regulation for only the health market, which privacy protection reference model is being used?

A. Co-regulatory
B. Sectoral
C. Comprehensive
D. Self-regulatory

Answer: C

NEW QUESTION 125
Which of the following helps define data retention time is a stream-fed data lake that includes personal data?

A. Information security assessments
B. Privacy impact assessments (PIAs)
C. Data privacy standards
D. Data lake configuration

Answer: B

NEW QUESTION 127
Which of the following is the PRIMARY reason that organizations need to map the data flows of personal data?

A. To assess privacy risks
B. To evaluate effectiveness of data controls
C. To determine data integration gaps
D. To comply with regulations

Answer: A

NEW QUESTION 130
Which of the following MOST effectively protects against the use of a network sniffer?

A. Network segmentation
B. Transport layer encryption
C. An intrusion detection system (IDS)

D. A honeypot environment

Answer: C

NEW QUESTION 134
What is the PRIMARY means by which an organization communicates customer rights as it relates to the use of their personal information?

A. Distributing a privacy rights policy
B. Mailing rights documentation to customers
C. Publishing a privacy notice
D. Gaining consent when information is collected

Answer: D

NEW QUESTION 137
Which of the following is the MOST important consideration when writing an organization's privacy policy?

A. Using a standardized business taxonomy
B. Aligning statements to organizational practices
C. Ensuring acknowledgment by the organization's employees
D. Including a development plan for personal data handling

Answer: B

NEW QUESTION 139
Which of the following BEST ensures a mobile application implementation will meet an organization's data security standards?

A. User acceptance testing (UAT)
B. Data classification
C. Privacy impact assessment (PIA)
D. Automatic dynamic code scan

Answer: C

NEW QUESTION 143
Which of the following is the BEST way to hide sensitive personal data that is in use in a data lake?

A. Data masking
B. Data truncation
C. Data encryption
D. Data minimization

Answer: A

NEW QUESTION 147
Which of the following would MOST effectively reduce the impact of a successful breach through a remote access solution?

A. Compartmentalizing resource access
B. Regular testing of system backups
C. Monitoring and reviewing remote access logs
D. Regular physical and remote testing of the incident response plan

Answer: D

NEW QUESTION 150
Which of the following should be the FIRST consideration when selecting a data sanitization method?

A. Risk tolerance
B. Implementation cost
C. Industry standards
D. Storage type

Answer: D

NEW QUESTION 153
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?

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: A

NEW QUESTION 157
Which of the following helps to ensure the identities of individuals in two-way communication are verified?

A. Virtual private network (VPN)
B. Transport Layer Security (TLS)
C. Mutual certificate authentication
D. Secure Shell (SSH)

Answer: C

NEW QUESTION 161
A new marketing application needs to use data from the organization's customer database. Prior to the application using the data, which of the following should be done FIRST?

A. Ensure the data loss prevention (DLP) tool is logging activity.
B. De-identify all personal data in the database.
C. Determine what data is required by the application.
D. Renew the encryption key to include the application.

Answer: C

NEW QUESTION 165
Which of the following should an IT privacy practitioner do FIRST following a decision to expand remote working capability to all employees due to a global pandemic?

A. Evaluate the impact resulting from this change.
B. Revisit the current remote working policies.
C. Implement a virtual private network (VPN) tool.
D. Enforce multi-factor authentication for remote access.

Answer: B

NEW QUESTION 169
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CDPSE Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CDPSE Product From:

https://www.2passeasy.com/dumps/CDPSE/

Money Back Guarantee

CDPSE Practice Exam Features:

* CDPSE Questions and Answers Updated Frequently

* CDPSE Practice Questions Verified by Expert Senior Certified Staff

* CDPSE Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* CDPSE Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year