Vendor: ISACA

Exam Code: CDPSE

Exam Name: Certified Data Privacy Solutions Engineer (CDPSE)

Version: DEMO

QUESTION 1
Which of the following is the GREATEST concern for an organization subject to cross-border data transfer regulations when using a cloud service provider to store and process data?

A. The service provider has denied the organization's request for right to audit.
B. Personal data stored on the cloud has not been anonymized.
C. The extent of the service provider's access to data has not been established.
D. The data is stored in a region with different data protection requirements.

Answer: D
Explanation:
Cross-border data transfer regulations are laws and rules that govern the movement of personal data across national or regional boundaries. They aim to protect the privacy rights and interests of the data subjects, and to ensure that their personal data are not subject to lower or incompatible standards of protection in other jurisdictions. Examples of cross-border data transfer regulations include the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Information Protection Law (PIPL) in China.
When an organization uses a cloud service provider to store and process data, it may face the risk of transferring personal data to a region with different data protection requirements, such as a region that has not been recognized as providing adequate or equivalent levels of protection by the original jurisdiction, or a region that has conflicting or incompatible laws or regulations with the original jurisdiction. This may result in the following consequences for the organization:
- It may violate the cross-border data transfer regulations of the original jurisdiction, and face legal sanctions, fines, or lawsuits from the regulators, customers, or data subjects.
- It may lose control or visibility over the personal data, and expose them to unauthorized or unlawful access, use, modification, or disclosure by the cloud service provider or third parties.
- It may compromise the trust and confidence of the customers and data subjects, and damage its reputation and competitiveness.
Therefore, an organization subject to cross-border data transfer regulations should carefully assess and manage the risks of using a cloud service provider to store and process data, and ensure that it has appropriate safeguards and mechanisms in place to protect the privacy of personal data across borders.

QUESTION 2
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: C
Explanation:
The greatest benefit of adopting data minimization practices is that the associated threat surface is reduced. Data minimization is a privacy principle that states that personal data should be adequate, relevant, and limited to what is necessary for the purposes for which they are processed. Data minimization helps to protect data privacy by reducing the amount and type of personal data that are collected, stored, processed, or shared by an organization. This in turn reduces the exposure of personal data to potential threats, such as unauthorized access, use, disclosure, modification, or loss.

QUESTION 3

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
Explanation:
Data mapping is the process of defining how data elements from different sources are related, transformed, and transferred to a common destination. Data mapping is the first step when developing an application link because it helps to ensure that the data exchanged between the API and the third-party application is consistent, accurate, and compatible. Data mapping also helps to identify any gaps, errors, or conflicts in the data and resolve them before the data transfer occurs.

QUESTION 4
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
Explanation:
One of the most common vulnerabilities that can compromise the access to personal information is end users using weak passwords. Weak passwords are passwords that are easy to guess, crack, or steal, such as passwords that are short, simple, common, or reused. Weak passwords can allow unauthorized or malicious parties to gain access to personal information and cause privacy breaches, leaks, or misuse. Multi-factor authentication is an effective way to mitigate this vulnerability, as it requires end users to provide more than one piece of evidence to verify their identity, such as something they know (e.g., password), something they have (e.g., token), or something they are (e.g., biometric). Multi-factor authentication makes it harder for attackers to bypass the authentication process and access personal information.

QUESTION 5
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: B
Explanation:
The principle of data minimization states that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. By using

only the data required by the application, the organization can reduce the amount of data that is collected, stored, processed and potentially exposed. This can also help the organization comply with privacy laws and regulations that require data minimization, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

QUESTION 6
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?

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

Answer: D
Explanation:
Lawfulness and fairness is a data protection principle that states that personal data should be processed in a lawful, fair, and transparent manner in relation to the data subject. This means that personal data should be collected and used for legitimate purposes that are specified and communicated to the data subject, and that respect the rights and interests of the data subject. By posting 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, an online business is applying the lawfulness and fairness principle. The online business is informing the customers about the purpose and scope of data collection, and obtaining their consent or legal basis for processing their personal data.

QUESTION 7
What type of personal information can be collected by a mobile application without consent?

A. Full name
B. Geolocation
C. Phone number
D. Accelerometer data

Answer: D
Explanation:
Accelerometer data is a type of personal information that can be collected by a mobile application without consent, according to some studies and reports. Accelerometer data measures the movement and orientation of the device, and can be used for various purposes, such as fitness tracking, gaming, navigation, and authentication. However, accelerometer data can also reveal sensitive information about the user's behavior, activity, location, and identity, without their knowledge or permission. For example, some researchers have shown that accelerometer data can be used to infer the user's gender, age, health condition, personality traits, and even passwords. Therefore, accelerometer data poses a significant privacy risk for mobile users, and there is a lack of clear and consistent regulations and guidelines on how to collect, use, and protect this type of data.

QUESTION 8
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: C
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.

QUESTION 9
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
Explanation:
Before using data from the organization'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 anonymized. 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 needed.

QUESTION 10
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: D

QUESTION 11

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: C
Explanation:
A raw zone is a zone within a data lake that contains unprocessed or unstructured data that is ingested from various sources without any transformation or validation. A raw zone may contain sensitive data that has not been identified or classified yet, such as personal data. Therefore, sensitive data in a raw zone should be encrypted or tokenized to protect its confidentiality and integrity. Encryption is a process of transforming data into an unreadable form using a secret key or algorithm. Tokenization is a process of replacing sensitive data with non-sensitive substitutes called tokens. Both encryption and tokenization help to prevent unauthorized or unlawful access, use, disclosure, or transfer of sensitive data in a raw zone.

QUESTION 12
Which of the following poses the GREATEST privacy risk for client-side application processing?

A. Failure of a firewall protecting the company network
B. An employee loading personal information on a company laptop
C. A remote employee placing communication software on a company server
D. A distributed denial of service attack (DDoS) on the company network

Answer: B
Explanation:
The greatest privacy risk for client-side application processing is an employee loading personal information on a company laptop. Client-side application processing refers to performing data processing operations on the user's device or browser, rather than on a server or cloud. This can improve performance and user experience, but also pose privacy risks if the user's device is lost, stolen, hacked, or infected with malware. An employee loading personal information on a company laptop is exposing that information to potential threats on the client-side, such as unauthorized access, use, disclosure, modification, or loss. Therefore, an organization should implement appropriate security measures to protect personal information on client-side devices, such as encryption, authentication, authorization, logging, monitoring, etc.

QUESTION 13
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
Explanation:
The primary consideration to ensure control of remote access is aligned to the privacy policy is that access is only granted to authorized users. This means that the organization should

implement and enforce policies and procedures to identify, authenticate, and authorize users who need to access personal data remotely, such as employees, contractors, or service providers. The organization should also define and communicate the roles and responsibilities of remote users, and the terms and conditions of remote access, such as the purpose, scope, duration, and security measures. By granting access only to authorized users, the organization can protect data privacy by preventing unauthorized or unnecessary access, use, disclosure, or transfer of personal data.

QUESTION 14
Which of the following scenarios poses the GREATEST risk to an organization from a privacy perspective?

A. The organization lacks a hardware disposal policy.
B. Emails are not consistently encrypted when sent internally.
C. Privacy training is carried out by a service provider.
D. The organization's privacy policy has not been reviewed in over a year.

Answer: A
Explanation:
The scenario that poses the greatest risk to an organization from a privacy perspective is that the organization lacks a hardware disposal policy. A hardware disposal policy is a policy that defines how the organization should dispose of or destroy hardware devices that contain or process personal data, such as laptops, servers, hard drives, USBs, etc. A hardware disposal policy should ensure that personal data is securely erased or overwritten before the hardware device is discarded, recycled, donated, or sold. A hardware disposal policy should also comply with the applicable privacy regulations and standards that govern data retention and destruction. By lacking a hardware disposal policy, the organization exposes personal data to potential threats, such as theft, loss, or unauthorized access, use, disclosure, or transfer.

QUESTION 15
Within a business continuity plan (BCP), which of the following is the MOST important consideration to ensure the ability to restore availability and access to personal data in the event of a data privacy incident?

A. Offline backup availability
B. Recovery time objective (RTO)
C. Recovery point objective (RPO)
D. Online backup frequency

Answer: C
Explanation:
Recovery point objective (RPO) is the maximum amount of data that can be lost or corrupted before it affects the ability to restore the normal operations of a business. RPO is measured by the time interval between the last valid backup and the occurrence of a data privacy incident. A lower RPO means less data loss and faster recovery, while a higher RPO means more data loss and slower recovery. Therefore, RPO is the most important consideration to ensure the ability to restore availability and access to personal data in the event of a data privacy incident, because it determines how frequently and thoroughly the personal data should be backed up and protected.

QUESTION 16
In which of the following should the data record retention period be defined and established?

A. Data record model
B. Data recovery procedures
C. Data quality standard
D. Data management plan

Answer: D
Explanation:
A data management plan is a document that describes how data will be collected, stored, processed, shared, and disposed of throughout the data lifecycle. A data management plan should include information such as the purpose and scope of data processing, the data sources and types, the data quality and integrity standards, the data security and privacy measures, the data retention and destruction periods, the data ownership and governance structure, etc. A data management plan should also align with the organization's privacy policies and applicable privacy regulations and standards. Therefore, a data management plan is where the data record retention period should be defined and established.

QUESTION 17
When tokenizing credit card data, what security practice should be employed with the original data before it is stored in a data lake?

A. Encoding
B. Backup
C. Encryption
D. Classification

Answer: C
Explanation:
Encryption is a security practice that transforms data into an unreadable format using a secret key or algorithm. Encryption protects the confidentiality and integrity of data, especially when they are stored in a data lake or other cloud-based storage systems. Encryption ensures that only authorized parties can access and use the original data, while unauthorized parties cannot decipher or modify the data without the key or algorithm. Encryption also helps to comply with data protection laws and regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), which require data controllers and processors to implement appropriate technical and organizational measures to safeguard personal data. The other options are less effective or irrelevant for securing the original data before storing them in a data lake. Encoding is a process of converting data from one format to another, such as base64 or hexadecimal. Encoding does not protect the data from unauthorized access or use, as it can be easily reversed without a key or algorithm. Backup is a process of creating a copy of data for recovery purposes, such as in case of data loss or corruption. Backup does not protect the data from unauthorized access or use, as it may create additional copies of sensitive data that need to be secured. Classification is a process of assigning labels or categories to data based on their sensitivity, value or risk level, such as public, confidential or restricted. Classification helps to identify and manage the data according to their security requirements, but it does not protect the data from unauthorized access or use by itself.

QUESTION 18
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
Explanation:
The data owner is the key stakeholder within an organization who should be responsible for approving the outcomes of a privacy impact assessment (PIA). A PIA is a systematic process of identifying and evaluating the potential privacy risks and impacts of a data processing activity or system. The data owner is the person who has the authority and accountability for the data processing activity or system, and who determines the purpose and means of the data processing. The data owner should approve the outcomes of a PIA, such as the risk assessment, the risk mitigation plan, and the residual risk level, to ensure that they are consistent with the business objectives and legal obligations of the data processing activity or system.

QUESTION 19
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: C
Explanation:
The best reason for a health organization to use desktop virtualization to implement stronger access control to systems containing patient records is that it can improve data integrity and reduce effort for privacy audits. Desktop virtualization is a technology that allows users to access a virtual desktop environment that is hosted on a remote server, rather than on their local device. Desktop virtualization can enhance data privacy by providing stronger access control to systems containing patient records, such as requiring authentication, authorization, encryption, logging, etc. Desktop virtualization can also improve data integrity by ensuring that patient records are stored and processed in a centralized and secure location, rather than on multiple devices that may be vulnerable to loss, theft, damage, or corruption. Desktop virtualization can also reduce effort for privacy audits by simplifying the management and monitoring of data privacy compliance across different devices and locations.

QUESTION 20
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: D
Explanation:
The best way for an organization to maintain the effectiveness of its privacy breach incident response plan is to conduct annual data privacy tabletop exercises. A data privacy tabletop exercise is a simulated scenario that tests the organization's ability to respond to a privacy breach incident, such as a data breach, leak, or misuse. A data privacy tabletop exercise involves key

stakeholders, such as the privacy office, the information security team, the legal counsel, the public relations team, etc., who role-play their actions and decisions based on the scenario. A data privacy tabletop exercise helps to evaluate and improve the organization's privacy breach incident response plan, such as identifying gaps or weaknesses, validating roles and responsibilities, verifying procedures and protocols, assessing communication and coordination, etc.

QUESTION 21
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: C
Explanation:
Following an established privacy framework is the most important step when developing an organizational data privacy program because it provides a structured and consistent approach to identify, assess, and manage privacy risks and compliance obligations. A privacy framework can also help to align the privacy program with the organization's strategic goals, values, and culture, as well as to communicate and demonstrate the privacy program's effectiveness to internal and external stakeholders. Some examples of established privacy frameworks are the NIST Privacy Framework, the ISO/IEC 27701:2019, and the AICPA Privacy Maturity Model.

QUESTION 22
Which of the following should be considered personal information?

A. Biometric records
B. Company address
C. University affiliation
D. Age

Answer: A
Explanation:
Biometric records are personal information that can be used to identify an individual based on their physical or behavioral characteristics, such as fingerprints, facial recognition, iris scans, voice patterns, etc. Biometric records are considered sensitive personal information that require special protection and consent from the data subject. Biometric records can be used for various purposes, such as authentication, identification, security, etc., but they also pose privacy risks, such as unauthorized access, use, disclosure, or transfer of biometric data.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**