Question: 1

What should be the PRIMARY consideration of a multinational organization deploying a user and entity behavior analytics (UEBA) tool to centralize the monitoring of anomalous employee behavior?

A. Cross-border data transfer
B. Support staff availability and skill set
C. User notification
D. Global public interest

Answer: A

Explanation:

The primary consideration of a multinational organization deploying a user and entity behavior analytics (UEBA) tool to centralize the monitoring of anomalous employee behavior is cross-border data transfer, because it may involve the transfer of personal data across different jurisdictions with different privacy laws and regulations. The organization needs to ensure that it complies with the applicable legal requirements and safeguards the privacy rights of its employees when transferring their data to a central location for analysis. The other options are secondary or operational considerations that may not have a significant impact on the privacy of the employees. Reference: CDPSE Exam Content Outline, Domain 2 – Privacy Architecture (Privacy Architecture Implementation), Task 3: Implement privacy solutions1. CDPSE Review Manual, Chapter 2 – Privacy Architecture, Section 2.4 – Cross-Border Data Transfer2. CDPSE Certified Data Privacy Solutions Engineer All-in-One Exam Guide, Chapter 2 – Privacy Architecture, Section 2.5 – Cross-Border Data Transfer3.

Question: 2

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: A

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. Reference: 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

Question: 3

Which of the following BEST represents privacy threat modeling methodology?

A. Mitigating inherent risks and threats associated with privacy control weaknesses
B. Systematically eliciting and mitigating privacy threats in a software architecture
C. Reliably estimating a threat actor’s ability to exploit privacy vulnerabilities
D. Replicating privacy scenarios that reflect representative software usage

Answer: B

E xpl anati on:

Privacy threat modeling is a methodology for identifying and mitigating privacy threats in a software architecture. It helps to ensure that privacy is considered in the design and development of software systems, and that privacy risks are minimized or eliminated. Privacy threat modeling typically involves the following steps: defining the scope and context of the system, identifying the data flows and data elements, identifying the privacy threats and their sources, assessing the impact and likelihood of the threats, and applying appropriate countermeasures to mitigate the threats. Reference: : CDPSE Review Manual (Digital Version), page 97

Question: 4

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?
A. Data archiving
B. Data storage
C. Data acquisition
D. Data input

Answer: A

E xpl anati on:

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.

Data archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Data archiving helps to reduce the cost and complexity of data storage, improve the performance and availability of data systems, and comply with data retention policies and regulations. Data archiving should document controls relating to periods of retention for personal data, such as the criteria for determining the retention period, the procedures for deleting or anonymizing data after the retention period expires, and the mechanisms for ensuring the integrity and security of archived data. Reference: : CDPSE Review Manual (Digital Version), page 123

Question: 5

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: D

E xpl anati on:

The best way to address the concern that data collected by a third-party vendor and provided back to the organization may not be protected according to the organization's privacy notice is to validate contract compliance. This means that the organization should verify that the third-party vendor is adhering to the terms and conditions of the contract, which should include clauses on data protection, privacy, and security. The contract should also specify the obligations and responsibilities of both parties regarding data collection, processing, storage, transfer, retention, and disposal. By validating contract compliance, the organization can ensure that the third-party vendor is following the same privacy standards and practices as the organization.
Reference:
ISACA, CDPSE Review Manual 2021, Chapter 2: Privacy Governance, Section 2.3: Third-Party Management, p. 51-52.
ISACA, Data Privacy Audit/Assurance Program, Control Objective 8: Third-Party Management, p. 14-151