Boost up Your Certification Score

IAPP
CIPT
Certified Information Privacy Technologist (CIPT)



For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/cipt

Latest Version: 6.0

Question: 1

Which of the following best illustrates an ethical concern, rather than a legal violation, related to the processing of personal data?

A. The personal data collected by an organization create more risks than benefits to the individual.
B. CCTV is installed in employee break rooms without notice or justification.
C. An organization repurposes collected data without updating consent.
D. Users are given clear options to delete or export their personal data.

Answer: A

Explanation:
CIPT distinguishes ethical risks from legal violations . Ethical questions arise when a practice:
May be legal
But conflicts with fairness, proportionality, or respect for individuals
Creates disproportionate harm , surveillance concerns, or power imbalance
Lacks transparency or fails the ethical test of “should we,” even if “we legally can”
Option A best represents this. It involves:
An imbalance where organizational benefits outweigh risks to individuals
No explicit legal violation stated
A classic privacy ethics scenario in the CIPT curriculum under:
Ethical data stewardship
Evaluating proportionality and fairness
Risk-benefit balancing in data practices
Why the other options do not fit the ethical-only category:
B. CCTV in break rooms without notice → This typically violates legal requirements for transparency, signage, and purpose limitation.
C. Repurposing data without updated consent → A direct violation of consent and purpose-limitation requirements under major privacy laws (GDPR, etc.).
D. Clear deletion/export options → This is good practice , supporting data subject rights.
Thus, the option that describes an ethical concern rather than a clear legal breach is:
➡ A

Question: 2

SCENARIO
WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider AmaZure, which provides SQL Databases and Artificial Intelligence services to WebTracker. The roles and responsibilities between the two companies have been formalized in a standard contract, which includes allocating the role of data controller to WebTracker.

Visit us at: https://www.examsboost.com/test/cipt

The CEO of WebTracker, Mr. Bond, would like to assess the effectiveness of AmaZure ' s privacy controls, and he recently decided to hire you as an independent auditor. The scope of the engagement is limited only to the marketing services provided by WebTracker, you will not be evaluating any internal data processing activity, such as HR or Payroll.
This ad-hoc audit was triggered due to a future partnership between WebTracker and SmartHome — a partnership that will not require any data sharing. SmartHome is based in the USA, and most recently has dedicated substantial resources to developing smart refrigerators that can suggest the recommended daily calorie intake based on DNA information. This and other personal data is collected by WebTracker.
To get an idea of the scope of work involved, you have decided to start reviewing the company ' s documentation and interviewing key staff to understand potential privacy risks.
The results of this initial work include the following notes:
There are several typos in the current privacy notice of WebTracker, and you were not able to find the privacy notice for SmartHome.
You were unable to identify all the sub-processors working for SmartHome. No subcontractor is indicated in the cloud agreement with AmaZure, which is responsible for the support and maintenance of the cloud infrastructure.
There are data flows representing personal data being collected from the internal employees of WebTracker, including an interface from the HR system.
Part of the DNA data collected by WebTracker was from employees, as this was a prototype approved by the CEO of WebTracker.
All the WebTracker and SmartHome customers are based in USA and Canada.
Which of the following issues is most likely to require an investigation by the Chief Privacy Officer (CPO) of WebTracker?

A. Data flows use encryption for data at rest, as defined by the IT manager.
B. AmaZure sends newsletter to WebTracker customers, as approved by the Marketing Manager.
C. Employees' personal data are being stored in a cloud HR system, as approved by the HR Manager.
D. File Integrity Monitoring is being deployed in SQL servers, as indicated by the IT Architect Manager.

Answer: B

Explanation:
In the given scenario, WebTracker Limited is migrating its IT infrastructure to the cloud provider AmaZure. As part of this, it is crucial to understand the privacy and security implications associated with AmaZure's role as the data processor while WebTracker remains the data controller. The issues highlighted in the scenario provide a comprehensive understanding of the privacy risks and responsibilities involved.
The key issues identified include:
Typos in the privacy notice of WebTracker.
Missing privacy notice for SmartHome.
Unidentified sub-processors working for SmartHome.
Internal data flows from HR systems collecting employee data.
DNA data collected from employees for prototyping.
Among these issues, the most likely to require an investigation by the Chief Privacy Officer (CPO) of WebTracker is the one involving AmaZure sending newsletters to WebTracker customers (Option B).

This activity directly involves customer data and could indicate potential unauthorized processing or misuse of personal data, which is a significant privacy concern.
Detailed Explanation:
Option A (Encryption for Data at Rest): While ensuring data is encrypted at rest is critical, it does not directly indicate a breach of privacy or misuse of personal data. It is more about data security and less about privacy controls.
Option B (AmaZure Sends Newsletter): This involves direct interaction with customer data. If AmaZure is sending newsletters to WebTracker's customers, it implies that customer data is being processed and possibly used for marketing purposes. This requires explicit consent from the data subjects and appropriate contractual agreements between WebTracker and AmaZure. Without proper oversight, this could lead to unauthorized data processing and potential violations of privacy regulations.
Option C (Employees' Personal Data in Cloud HR System): Storing employee personal data in a cloud HR system, while significant, is typically within the scope of internal data processing. This issue is more about ensuring internal compliance with privacy policies rather than an immediate risk requiring CPO investigation.
Option D (File Integrity Monitoring in SQL Servers): File integrity monitoring is a security measure to ensure data integrity and does not directly indicate any privacy risks or misuse of personal data.
[References:, GDPR Articles 28 and 29 on the responsibilities of data controllers and processors., The necessity for explicit consent for data processing (GDPR Article 7)., Contractual obligations for data processors to protect personal data (GDPR Article 28)., Conclusion: The scenario of AmaZure sending newsletters to WebTracker customers (Option B) poses the most immediate and significant risk that requires an investigation by the CPO to ensure compliance with privacy regulations and avoid unauthorized use of customer data., ,]

Question: 3

SCENARIO
It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card. You are led down a long corridor with server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain
Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.
"We were hacked twice last year," Dr. Batch says, "and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again." She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.
You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself

considering an intriguing question Can these people be sure that I am who I say I am? You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key. Still pondering, you attempt to pull up the facility ' s wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found.
Why would you recommend that GFC use record encryption rather than disk, file or table encryption?

A. Record encryption is asymmetric, a stronger control measure.
B. Record encryption is granular, limiting the damage of potential breaches.
C. Record encryption involves tag masking, so its metadata cannot be decrypted
D. Record encryption allows for encryption of personal data only.

Answer: B

Explanation:
Record encryption provides a more granular level of security compared to disk, file, or table encryption. It encrypts individual records within a database, which means that even if a breach occurs, the exposure is limited to the specific records accessed rather than the entire database or table. This granular approach minimizes the potential damage and data loss in case of a security breach. Additionally, it allows for more precise control over access and decryption, enhancing overall security measures within the facility.

Question: 4

A healthcare provider would like to data mine information for research purposes however the Chief Privacy Officer is concerned medical data of individuals may be disclosed overcome the concern, which is the preferred technique for protecting such data while still allowing for analysis?

A. Access Control
B. Encryption
C. Isolation
D. Perturbation

Answer: D

Explanation:
Perturbation is the preferred technique for protecting medical data while still allowing for analysis. Perturbation involves adding noise to the data to prevent the identification of individuals while preserving the overall patterns and trends in the dataset. This method is particularly useful in data mining for research purposes where privacy concerns must be addressed. The IAPP's CIPT materials cover this technique under data anonymization and de-identification strategies, emphasizing its importance in research and analytics.

Question: 5

What Privacy by Design (PbD) element should include a de-identification or deletion plan?

A. Categorization.
B. Remediation.
C. Retention.
D. Security

Answer: C

Explanation:
• Privacy by Design (PbD) Principles: PbD emphasizes the proactive inclusion of privacy in the design and operation of IT systems, networks, and business practices.
• Retention: The retention element in PbD involves specifying the duration for which personal data will be retained. This is crucial to ensure that data is not kept longer than necessary.
• De-identification or Deletion: As part of the retention plan, organizations must decide on de-identifying or deleting personal data once it is no longer needed for its original purpose. This practice minimizes privacy risks associated with unnecessary data retention.
• Reference: According to the IAPP ' s " Privacy by Design: The 7 Foundational Principles, " the principle of retention emphasizes that personal data should be retained only as long as necessary to fulfill the specified purposes and that secure deletion or de-identification procedures should be implemented.

Question: 6

A privacy technologist works at a company operating in a jurisdiction where customers have the right to have their personal data erased. What are the most important technological controls that the privacy technologist needs to implement to ensure personal data can be deleted?

A. Data discovery tools to identify where data resides.
B. Automated deletion tools to ensure efficiency and consistency.
C. Audit trails to track deletion requests and actions.
D. User-facing deletion tools to empower users to manage their own data.

Answer: A

Explanation:
CIPT emphasizes that data discovery and mapping is the foundational prerequisite to honoring the right to erasure (right to be forgotten).
A company cannot delete what it cannot locate.
Data discovery tools allow a privacy technologist to:
Identify all systems, databases, logs, backups, and replicas where personal data exists
Map structured and unstructured data stores
Ensure downstream and third-party copies are detected
Enable accurate, complete, and lawful erasure across the data lifecycle
This directly aligns with:
CIPT's Data Lifecycle Management training
ISO/IEC 27701 requirements for knowing data locations
GDPR Article 17 (erasure) expectations

NIST Privacy Framework: Data Processing Ecosystem Mapping
Why other options are not the most important control:
B — Automated deletion tools: Useful but impossible to implement correctly without knowing where data resides .
C — Audit trails: Essential for accountability, but they do not ensure data can be deleted.
D — User-facing deletion tools: Important but only act on front-end processes, not system-wide deletion.

Question: 7

An individual drives to a grocery store to buy food for dinner. When she arrives, she receives several unsolicited notifications on her phone about discounts on items in the store. Which type of privacy problem does this represent?

A. Intrusion.
B. Surveillance.
C. Decisional Interference.
D. Exposure.

Answer: A

Explanation:
CIPT describes privacy harms based on Solove's Privacy Taxonomy. "Intrusion" refers to disturbances or interruptions that invade a person's private life , including:
Unwanted communications
Targeted advertising without user expectation
Push notifications or messages based on location or behavior
The situation clearly meets the definition of intrusion because:
The user receives unsolicited , unexpected messages
The notifications are triggered by location-based tracking , causing disturbance
The user did not request or initiate such contact
CIPT points out that intrusive practices often result from:
Over-collection of behavioral/location data
Failure to respect contextual privacy expectations
Poor consent or preference management mechanisms
Why the other options are incorrect:
B — Surveillance: Involves continuous or systematic monitoring, not a one-time targeted notification.
C — Decisional Interference: Involves influencing or manipulating personal decisions (e.g., limiting free choice) — not the case here.
D — Exposure: Relates to revealing personal information publicly — not applicable here.

Question: 8

Which is NOT a suitable action to apply to data when the retention period ends?

A. Aggregation.
B. De-identification.
C. Deletion.
D. Retagging.

Answer: D

Explanation:
When the retention period for data ends, suitable actions typically include deletion, de-identification, or aggregation to ensure that the data is no longer in a form that can be used to identify individuals or is completely removed from systems. Retagging is not a suitable action as it implies merely re-labeling or reclassifying the data rather than properly handling it according to data retention policies. Retagging does not mitigate privacy risks and may result in non-compliance with data protection regulations (IAPP, Certified Information Privacy Technologist (CIPT) materials).

Question: 9

An organization is concerned that its aging IT infrastructure will lead to Increased security and privacy risks. Which of the following would help mitigate these risks?

A. Vulnerability management.
B. Data Loss Prevention.
C. Code audits.
D. Network Centricity.

Answer: A

Explanation:
To mitigate the security and privacy risks associated with an aging IT infrastructure, vulnerability management is essential. This process involves identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. Regular vulnerability assessments and management ensure that any weaknesses are promptly addressed, reducing the risk of exploitation. Other options, like Data Loss Prevention, Code Audits, and Network Centricity, while useful, are not as directly targeted at the overarching issue of managing vulnerabilities in aging systems. (Reference: IAPP CIPT Study Guide, Chapter on Risk Management and Security Controls)

Question: 10

To meet data protection and privacy legal requirements that may require personal data to be disposed of or deleted when no longer necessary for the use it was collected, what is the best privacy-enhancing solution a privacy technologist should recommend be implemented in application design to meet this requirement?

A. Implement a process to delete personal data on demand and maintain records on deletion requests.
B. Implement automated deletion of off-site backup of personal data based on annual risk assessments.

C. Develop application logic to validate and purge personal data according to legal hold status or retention schedule.
D. Securely archive personal data not accessed or used in the last 6 months. Automate a quarterly review to delete data from archive once no longer needed.

Answer: C

Explanation:
To meet data protection and privacy legal requirements regarding the disposal or deletion of personal data when it is no longer necessary, the best privacy-enhancing solution involves integrating robust application logic. Option C suggests developing application logic that validates and purges personal data according to its legal hold status or retention schedule. This approach ensures compliance with legal mandates for data retention and deletion, minimizing the risk of retaining unnecessary personal data. References to this can be found in IAPP's CIPT materials, specifically in the sections discussing data lifecycle management and legal compliance requirements.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer

