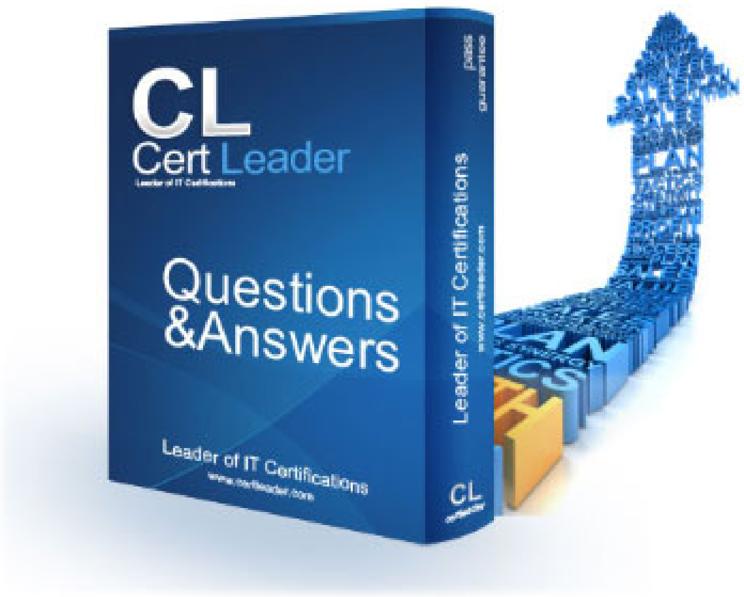
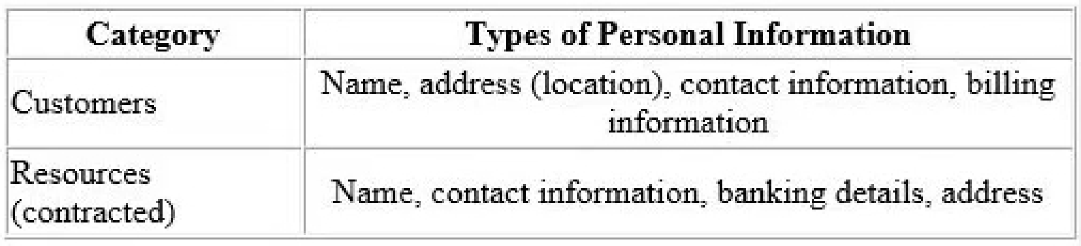
CIPT Dumps

Certified Information Privacy Technologist

https://www.certleader.com/CIPT-dumps.html



NEW QUESTION 1
SCENARIO
Clean-Q is a company that offers house-hold and office cleaning services. The company receives requests from consumers via their website and telephone, to book cleaning services. Based on the type and size of service, Clean-Q then contracts individuals that are registered on its resource database - currently managed in-house by Clean-Q IT Support. Because of Clean-Q's business model, resources are contracted as needed instead of permanently employed.
The table below indicates some of the personal information Clean-Q requires as part of its business operations:



Category	Types of Personal Information
Customers	Name, address (location), contact information, billing information
Resources (contracted)	Name, contact information, banking details, address

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.
With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings.
Ina business strategy session held by senior management recently, Clear-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q’s solution providers, presenting their proposed solutions and platforms.
The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.

- A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
- A resource facing web interface that enables resources to apply and manage their assigned jobs.
- An online payment facility for customers to pay for services.

Which question would you most likely ask to gain more insight about LeadOps and provide practical privacy recommendations?

A. What is LeadOps’ annual turnover?
B. How big is LeadOps’ employee base?
C. Where are LeadOps' operations and hosting services located?
D. Does LeadOps practice agile development and maintenance of their system?

Answer: D

NEW QUESTION 2
Which is the most accurate type of biometrics?

A. DNA
B. Voiceprint.
C. Fingerprint.
D. Facial recognition.

Answer: B

NEW QUESTION 3
Implementation of privacy controls for compliance with the requirements of the Children’s Online Privacy Protection Act (COPPA) is necessary for all the following situations EXCEPT?

A. A virtual jigsaw puzzle game marketed for ages 5-9 displays pieces of the puzzle on a handheld screen.Once the child completes a certain level, it flashes a message about new themes released that day.
B. An interactive toy copies a child’s behavior through gestures and kid-friendly sound
C. It runs on battery power and automatically connects to a base station at home to charge itself.
D. A math tutoring service commissioned an advertisement on a bulletin board inside a charter schoo
E. The service makes it simple to reach out to tutors through a QR-code shaped like a cartoon character.
F. A note-taking application converts hard copies of kids’ class notes into audio books in second
G. It does so by using the processing power of idle server farms.

Answer: A

NEW QUESTION 4
What is the main reason a company relies on implied consent instead of explicit consent from a user to process her data?

A. The implied consent model provides the user with more detailed data collection information.
B. To secure explicit consent, a user's website browsing would be significantly disrupted.
C. An explicit consent model is more expensive to implement.
D. Regulators prefer the implied consent model.

Answer: A

NEW QUESTION 5
Properly configured databases and well-written website codes are the best protection against what online threat?

A. Pharming.
B. SQL injection.
C. Malware execution.

D. System modification.

Answer: B

NEW QUESTION 6
What must be done to destroy data stored on "write once read many" (WORM) media?

A. The data must be made inaccessible by encryption.
B. The erase function must be used to remove all data.
C. The media must be physically destroyed.
D. The media must be reformatted.

Answer: C

NEW QUESTION 7
Which is NOT a drawback to using a biometric recognition system?

A. It can require more maintenance and support.
B. It can be more expensive than other systems
C. It has limited compatibility across systems.
D. It is difficult for people to use.

Answer: A

NEW QUESTION 8
Which of the following would best improve an organization’ s system of limiting data use?

A. Implementing digital rights management technology.
B. Confirming implied consent for any secondary use of data.
C. Applying audit trails to resources to monitor company personnel.
D. Instituting a system of user authentication for company personnel.

Answer: C

NEW QUESTION 9
Which of the following statements is true regarding software notifications and agreements?

A. Website visitors must view the site’s privacy statement before downloading software.
B. Software agreements are designed to be brief, while notifications provide more details.
C. It is a good practice to provide users with information about privacy prior to software installation.
D. “Just in time” software agreement notifications provide users with a final opportunity to modify the agreement.

Answer: C

NEW QUESTION 10
In the realm of artificial intelligence, how has deep learning enabled greater implementation of machine learning?

A. By using hand-coded classifiers like edge detection filters so that a program can identify where an object starts and stops.
B. By increasing the size of neural networks and running massive amounts of data through the network to train it.
C. By using algorithmic approaches such as decision tree learning and inductive logic programming.
D. By hand coding software routines with a specific set of instructions to accomplish a task.

Answer: B

NEW QUESTION 10
Under the Family Educational Rights and Privacy Act (FERPA), releasing personally identifiable information from a student's educational record requires written permission from the parent or eligible student in order for information to be?

A. Released to a prospective employer.
B. Released to schools to which a student is transferring.
C. Released to specific individuals for audit or evaluation purposes.
D. Released in response to a judicial order or lawfully ordered subpoena.

Answer: C

NEW QUESTION 12
What term describes two re-identifiable data sets that both come from the same unidentified individual?

A. Pseudonymous data.
B. Anonymous data.
C. Aggregated data.
D. Imprecise data.

Answer: B

NEW QUESTION 17
SCENARIO
Looking back at your first two years as the Director of Personal Information Protection and Compliance for the Berry Country Regional Medical Center in Thorn Bay, Ontario, Canada, you see a parade of accomplishments, from developing state-of-the-art simulation based training for employees on privacy protection to establishing an interactive medical records system that is accessible by patients as well as by the medical personnel. Now, however, a question you have put off looms large: how do we manage all the
data-not only records produced recently, but those still on hand from years ago? A data flow diagram generated last year shows multiple servers, databases, and work stations, many of which hold files that have not yet been incorporated into the new records system. While most of this data is encrypted, its persistence may pose security and compliance concerns. The situation is further complicated by several long-term studies being conducted by the medical staff using patient information. Having recently reviewed the major Canadian privacy regulations, you want to make certain that the medical center is observing them.
You also recall a recent visit to the Records Storage Section, often termed “The Dungeon” in the basement of the old hospital next to the modern facility, where you noticed a multitude of paper records. Some of these were in crates marked by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. The back shelves of the section housed data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the dungeon, you noticed just ahead of you a small man in a lab coat who you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.
Which cryptographic standard would be most appropriate for protecting patient credit card information in the records system?

A. Asymmetric Encryption
B. Symmetric Encryption
C. Obfuscation
D. Hashing

Answer: A

NEW QUESTION 18
A vendor has been collecting data under an old contract, not aligned with the practices of the organization. Which is the preferred response?

A. Destroy the data
B. Update the contract to bring the vendor into alignment.
C. Continue the terms of the existing contract until it expires.
D. Terminate the contract and begin a vendor selection process.

Answer: B

NEW QUESTION 22
SCENARIO
Please use the following to answer the next question:
Chuck, a compliance auditor for a consulting firm focusing on healthcare clients, was required to travel to the client’s office to perform an onsite review of the client’s operations. He rented a car from Finley Motors upon arrival at the airport as so he could commute to and from the client’s office. The car rental agreement was electronically signed by Chuck and included his name, address, driver’s license, make/model of the car, billing rate, and additional details describing the rental transaction. On the second night, Chuck was caught by a red light camera not stopping at an intersection on his way to dinner. Chuck returned the car back to the car rental agency at the end week without mentioning the infraction and Finley Motors emailed a copy of the final receipt to the address on file.
Local law enforcement later reviewed the red light camera footage. As Finley Motors is the registered owner of the car, a notice was sent to them indicating the infraction and fine incurred. This notice included the license plate number, occurrence date and time, a photograph of the driver, and a web portal link to a video clip of the violation for further review. Finley Motors, however, was not responsible for the violation as they were not driving the car at the time and transferred the incident to AMP Payment Resources for further review. AMP Payment Resources identified Chuck as the driver based on the rental agreement he signed when picking up the car and then contacted Chuck directly through a written letter regarding the infraction to collect the fine.
After reviewing the incident through the AMP Payment Resources’ web portal, Chuck paid the fine using his personal credit card. Two weeks later, Finley Motors sent Chuck an email promotion offering 10% off a future rental.
How can Finley Motors reduce the risk associated with transferring Chuck’s personal information to AMP Payment Resources?

A. By providing only the minimum necessary data to process the violation notice and masking all other information prior to transfer.
B. By requesting AMP Payment Resources delete unnecessary datasets and only utilize what is necessary to process the violation notice.
C. By obfuscating the minimum necessary data to process the violation notice and require AMP Payment Resources to secure store the personal information.
D. By transferring all information to separate datafiles and requiring AMP Payment Resources to combine the datasets during processing of the violation notice.

Answer: A

NEW QUESTION 23
A credit card with the last few numbers visible is an example of what?

A. Masking data
B. Synthetic data
C. Sighting controls.
D. Partial encryption

Answer: A

NEW QUESTION 24
An organization based in California, USA is implementing a new online helpdesk solution for recording customer call information. The organization considers the capture of personal data on the online helpdesk solution to be in the interest of the company in best servicing customer calls.
Before implementation, a privacy technologist should conduct which of the following?

A. A Data Protection Impact Assessment (DPIA) and consultation with the appropriate regulator to ensure legal compliance.
B. A privacy risk and impact assessment to evaluate potential risks from the proposed processing operations.
C. A Legitimate Interest Assessment (LIA) to ensure that the processing is proportionate and does not override the privacy, rights and freedoms of the customers.
D. A security assessment of the help desk solution and provider to assess if the technology was developed with a security by design approach.

Answer: C

NEW QUESTION 26
Which of the following is a vulnerability of a sensitive biometrics authentication system?

A. False positives.
B. False negatives.
C. Slow recognition speeds.
D. Theft of finely individualized personal data.

Answer: C

NEW QUESTION 31
Value Sensitive Design (VSD) focuses on which of the following?

A. Quality and benefit.
B. Ethics and morality.
C. Principles and standards.
D. Privacy and human rights.

Answer: C

NEW QUESTION 33
What is the potential advantage of homomorphic encryption?

A. Encrypted information can be analyzed without decrypting it first.
B. Ciphertext size decreases as the security level increases.
C. It allows greater security and faster processing times.
D. It makes data impenetrable to attacks.

Answer: C

NEW QUESTION 37
What is the main benefit of using dummy data during software testing?

A. The data comes in a format convenient for testing.
B. Statistical disclosure controls are applied to the data.
C. The data enables the suppression of particular values in a set.
D. Developers do not need special privacy training to test the software.

Answer: D

NEW QUESTION 39
A key principle of an effective privacy policy is that it should be?

A. Written in enough detail to cover the majority of likely scenarios.
B. Made general enough to maximize flexibility in its application.
C. Presented with external parties as the intended audience.
D. Designed primarily by the organization's lawyers.

Answer: C

NEW QUESTION 41
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.
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.

Based on the initial assessment and review of the available data flows, which of the following would be the most important privacy risk you should investigate first?

A. Verify that WebTracker's HR and Payroll systems implement the current privacy notice (after the typos are fixed).
B. Review the list of subcontractors employed by AmaZure and ensure these are included in the formal agreement with WebTracker.
C. Evaluate and review the basis for processing employees' personal data in the context of the prototype created by WebTracker and approved by the CEO.

D. Confirm whether the data transfer from London to the USA has been fully approved by AmaZure and the appropriate institutions in the USA and the European Union.

Answer: C

NEW QUESTION 43
What is the main reason the Do Not Track (DNT) header is not acknowledged by more companies?

A. Most web browsers incorporate the DNT feature.
B. The financial penalties for violating DNT guidelines are too high.
C. There is a lack of consensus about what the DNT header should mean.
D. It has been difficult to solve the technological challenges surrounding DNT.

Answer: C

NEW QUESTION 47
SCENARIO
Please use the following to answer the next question:
Jordan just joined a fitness-tracker start-up based in California, USA, as its first Information Privacy and Security Officer. The company is quickly growing its business but does not sell any of the fitness trackers itself. Instead, it relies on a distribution network of third-party retailers in all major countries. Despite not having any stores, the company has a 78% market share in the EU. It has a website presenting the company and products, and a member section where customers can access their information. Only the email address and physical address need to be provided as part of the registration process in order to customize the site to the user's region and country. There is also a newsletter sent every month to all members featuring fitness tips, nutrition advice, product spotlights from partner companies based on user behavior and preferences.
Jordan says the General Data Protection Regulation (GDPR) does not apply to the company. He says the company is not established in the EU, nor does it have a processor in the region. Furthermore, it does not do any "offering goods or services" in the EU since it does not do any marketing there, nor sell to consumers directly. Jordan argues that it is the customers who chose to buy the products on their own initiative and there is no "offering" from the company.
The fitness trackers incorporate advanced features such as sleep tracking, GPS tracking, heart rate monitoring. wireless syncing, calorie-counting and step-tracking. The watch must be paired with either a smartphone or a computer in order to collect data on sleep levels, heart rates, etc. All information from the device must be sent to the company's servers in order to be processed, and then the results are sent to the smartphone or computer. Jordan argues that there is no personal information involved since the company does not collect banking or social security information.
Based on the current features of the fitness watch, what would you recommend be implemented into each device in order to most effectively ensure privacy?

A. Hashing.
B. A2DP Bluetooth profile.
C. Persistent unique identifier.
D. Randomized MAC address.

Answer: C

NEW QUESTION 49
Which of the following most embodies the principle of Data Protection by Default?

A. A messaging app for high school students that uses HTTPS to communicate with the server.
B. An electronic teddy bear with built-in voice recognition that only responds to its owner's voice.
C. An internet forum for victims of domestic violence that allows anonymous posts without registration.
D. A website that has an opt-in form for marketing emails when registering to download a whitepaper.

Answer: D

NEW QUESTION 53
Which of the following entities would most likely be exempt from complying with the General Data Protection Regulation (GDPR)?

A. A South American company that regularly collects European customers' personal data.
B. A company that stores all customer data in Australia and is headquartered in a European Union (EU) member state.
C. A Chinese company that has opened a satellite office in a European Union (EU) member state to service European customers.
D. A North American company servicing customers in South Africa that uses a cloud storage system made by a European company.

Answer: C

NEW QUESTION 55
What is typically NOT performed by sophisticated Access Management (AM) techniques?

A. Restricting access to data based on location.
B. Restricting access to data based on user role.
C. Preventing certain types of devices from accessing data.
D. Preventing data from being placed in unprotected storage.

Answer: B

NEW QUESTION 58
SCENARIO
Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company's information security policy and industry standards. Kyle is also new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle's schedule included participating in meetings and observing work in the IT and compliance departments.
Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to

Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization's wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.
Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company's privacy risk assessment, noting that the secondary use of personal information was considered a high risk.
By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn't wait to recommend his friend Ben who would be perfect for the job.
Which data practice is Barney most likely focused on improving?

A. Deletion
B. Inventory.
C. Retention.
D. Sharing

Answer: C

NEW QUESTION 63
What distinguishes a "smart" device?

A. It can perform multiple data functions simultaneously.
B. It is programmable by a user without specialized training.
C. It can reapply access controls stored in its internal memory.
D. It augments its intelligence with information from the internet.

Answer: D

NEW QUESTION 66
Organizations understand there are aggregation risks associated with the way the process their customer's data. They typically include the details of this aggregation risk in a privacy notice and ask that all customers acknowledge they understand these risks and consent to the processing.
What type of risk response does this notice and consent represent?

A. Risk transfer.
B. Risk mitigation.
C. Risk avoidance.
D. Risk acceptance.

Answer: A

NEW QUESTION 69
SCENARIO
Please use the following to answer next question:
EnsureClaim is developing a mobile app platform for managing data used for assessing car accident insurance claims. Individuals use the app to take pictures at the crash site, eliminating the need for a built-in vehicle camera. EnsureClaim uses a third-party hosting provider to store data collected by the app. EnsureClaim customer service employees also receive and review app data before sharing with insurance claim adjusters.
The app collects the following information: First and last name
Date of birth (DOB) Mailing address Email address
Car VIN number Car model License plate
Insurance card number Photo
Vehicle diagnostics Geolocation
The app is designed to collect and transmit geolocation data. How can data collection best be limited to the necessary minimum?

A. Allow user to opt-out geolocation data collection at any time.
B. Allow access and sharing of geolocation data only after an accident occurs.
C. Present a clear and explicit Explanation about need for the geolocation data.
D. Obtain consent and capture geolocation data at all times after consent is received.

Answer: D

NEW QUESTION 74
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.
What measures can protect client information stored at GFDC?

A. De-linking of data into client-specific packets.
B. Cloud-based applications.
C. Server-side controls.
D. Data pruning

Answer: A

NEW QUESTION 78
All of the following can be indications of a ransomware attack EXCEPT?

A. The inability to access certain files.
B. An increased amount of spam email in an individual's inbox.
C. An increase in activity of the CPU of a computer for no apparent reason.
D. The detection of suspicious network communications between the ransomware and the attacker's command and control servers.

Answer: B

NEW QUESTION 80
Which of the following statements best describes the relationship between privacy and security?

A. Security systems can be used to enforce compliance with privacy policies.
B. Privacy and security are independent; organizations must decide which should by emphasized.
C. Privacy restricts access to personal information; security regulates how information should be used.
D. Privacy protects data from being viewed during collection and security governs how collected data should be shared.

Answer: C

NEW QUESTION 83
What is the main benefit of using a private cloud?

A. The ability to use a backup system for personal files.
B. The ability to outsource data support to a third party.
C. The ability to restrict data access to employees and contractors.
D. The ability to cut costs for storing, maintaining, and accessing data.

Answer: C

NEW QUESTION 88
How does k-anonymity help to protect privacy in micro data sets?

A. By ensuring that every record in a set is part of a group of "k" records having similar identifying information.
B. By switching values between records in order to preserve most statistics while still maintaining privacy.
C. By adding sufficient noise to the data in order to hide the impact of any one individual.
D. By top-coding all age data above a value of "k."

Answer: A

NEW QUESTION 91
SCENARIO
Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company's information security policy and industry standards. Kyle is also new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle's schedule included participating in meetings and observing work in the IT and compliance departments.
Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization's wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.
Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company's privacy risk assessment, noting that the secondary use of personal information was considered a high risk.
By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn't wait to recommend his friend Ben who would be perfect for the job.
Which of the following should Kyle recommend to Jill as the best source of support for her initiative?

A. Investors.
B. Regulators.
C. Industry groups.
D. Corporate researchers.

Answer: C

NEW QUESTION 96
Which of the following is considered a client-side IT risk?

A. Security policies focus solely on internal corporate obligations.
B. An organization increases the number of applications on its server.
C. An employee stores his personal information on his company laptop.
D. IDs used to avoid the use of personal data map to personal data in another database.

Answer: C

NEW QUESTION 100
You are a wine collector who uses the web to do research about your hobby. You navigate to a news site and an ad for wine pops up. What kind of advertising is this?

A. Remnant.
B. Behavioral.
C. Contextual.
D. Demographic.

Answer: B

NEW QUESTION 104
Users of a web-based email service have their accounts breached through compromised login credentials. Which possible consequences of the breach illustrate the two categories of Calo's Harm Dimensions?

A. Financial loss and blackmail.
B. Financial loss and solicitation.
C. Identity theft and embarrassment.
D. Identity theft and the leaking of information.

Answer: D

NEW QUESTION 108
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.
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

NEW QUESTION 113
Which of the following became a foundation for privacy principles and practices of countries and organizations across the globe?

A. The Personal Data Ordinance.
B. The EU Data Protection Directive.
C. The Code of Fair Information Practices.
D. The Organization for Economic Co-operation and Development (OECD) Privacy Principles.

Answer: D

NEW QUESTION 117
A privacy engineer has been asked to review an online account login page. He finds there is no limitation on the number of invalid login attempts a user can make when logging into their online account.
What would be the best recommendation to minimize the potential privacy risk from this weakness?

A. Implement a CAPTCHA system.
B. Develop server-side input validation checks.
C. Enforce strong password and account credentials.

D. Implement strong Transport Layer Security (TLS) to ensure an encrypted link.

Answer: B

NEW QUESTION 119
After committing to a Privacy by Design program, which activity should take place first?

A. Create a privacy standard that applies to all projects and services.
B. Establish a retention policy for all data being collected.
C. Implement easy to use privacy settings for users.
D. Perform privacy reviews on new projects.

Answer: B

NEW QUESTION 122
Which of the following would be the most appropriate solution for preventing privacy violations related to information exposure through an error message?

A. Configuring the environment to use shorter error messages.
B. Handing exceptions internally and not displaying errors to the user.
C. Creating default error pages or error messages which do not include variable data.
D. Logging the session name and necessary parameters once the error occurs to enable trouble shooting.

Answer: C

NEW QUESTION 125
SCENARIO
You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.
Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells online through retail sites designated for industries and demographics, sites such as “My Cool Ride" for automobile-related products or “Zoomer” for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.
You have been asked to lead three important new projects at Ancillary:
The first is the personal data management and security component of a multi-faceted initiative to unify the company’s culture. For this project, you are considering using a series of third- party servers to provide company data and approved applications to employees.
The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.
Finally, you are charged with developing privacy protections for a single web store housing all the company’s product lines as well as products from affiliates. This new omnibus site will be known, aptly, as “Under the Sun.” The Director of Marketing wants the site not only to sell Ancillary’s products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.
If you are asked to advise on privacy concerns regarding paid advertisements, which is the most important aspect to cover?

A. Unseen web beacons that combine information on multiple users.
B. Latent keys that trigger malware when an advertisement is selected.
C. Personal information collected by cookies linked to the advertising network.
D. Sensitive information from Structured Query Language (SQL) commands that may be exposed.

Answer: C

NEW QUESTION 128
Which of the following provides a mechanism that allows an end-user to use a single sign-on (SSO) for multiple services?

A. The Open ID Federation.
B. PCI Data Security Standards Council
C. International Organization for Standardization.
D. Personal Information Protection and Electronic Documents Act.

Answer: A

NEW QUESTION 129
After downloading and loading a mobile app, the user is presented with an account registration page requesting the user to provide certain personal details. Two statements are also displayed on the same page along with a box for the user to check to indicate their confirmation:
Statement 1 reads: “Please check this box to confirm you have read and accept the terms and conditions of the end user license agreement” and includes a hyperlink to the terms and conditions.
Statement 2 reads: “Please check this box to confirm you have read and understood the privacy notice” and includes a hyperlink to the privacy notice.
Under the General Data Protection Regulation (GDPR), what lawful basis would you primarily except the privacy notice to refer to?

A. Consent.
B. Vital interests.
C. Legal obligation.
D. Legitimate interests.

Answer: A

NEW QUESTION 131
SCENARIO
Looking back at your first two years as the Director of Personal Information Protection and Compliance for the Berry Country Regional Medical Center in Thorn Bay, Ontario, Canada, you see a parade of accomplishments, from developing state-of-the-art simulation based training for employees on privacy protection to establishing an interactive medical records system that is accessible by patients as well as by the medical personnel. Now, however, a question you have put off looms large: how do we manage all the
data-not only records produced recently, but those still on hand from years ago? A data flow diagram generated last year shows multiple servers, databases, and work stations, many of which hold files that have not yet been incorporated into the new records system. While most of this data is encrypted, its persistence may pose security and compliance concerns. The situation is further complicated by several long-term studies being conducted by the medical staff using patient information. Having recently reviewed the major Canadian privacy regulations, you want to make certain that the medical center is observing them.
You also recall a recent visit to the Records Storage Section, often termed "The Dungeon" in the basement of the old hospital next to the modern facility, where you noticed a multitude of paper records. Some of these were in crates marked by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. The back shelves of the section housed data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the dungeon, you noticed just ahead of you a small man in a lab coat who you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.
Which data lifecycle phase needs the most attention at this Ontario medical center?

A. Retention
B. Disclosure
C. Collection
D. Use

Answer: A

NEW QUESTION 133
SCENARIO
Please use the following to answer next question:
EnsureClaim is developing a mobile app platform for managing data used for assessing car accident insurance claims. Individuals use the app to take pictures at the crash site, eliminating the need for a built-in vehicle camera. EnsureClaim uses a third-party hosting provider to store data collected by the app. EnsureClaim customer service employees also receive and review app data before sharing with insurance claim adjusters.
The app collects the following information: First and last name
Date of birth (DOB) Mailing address Email address
Car VIN number Car model License plate
Insurance card number Photo
Vehicle diagnostics
Geolocation
All of the following technical measures can be implemented by EnsureClaim to protect personal information that is accessible by third-parties EXCEPT?

A. Encryption.
B. Access Controls.
C. De-identification.
D. Multi-factor authentication.

Answer: B

NEW QUESTION 134
Which of the following modes of interaction often target both people who personally know and are strangers to the attacker?

A. Spam.
B. Phishing.
C. Unsolicited sexual imagery.
D. Consensually-shared sexual imagery.

Answer: B

NEW QUESTION 139
SCENARIO
You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.
Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells online through retail sites designated for industries and demographics, sites such as "My Cool Ride" for automobile-related products or "Zoomer" for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.
You have been asked to lead three important new projects at Ancillary:
The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third- party servers to provide company data and approved applications to employees.
The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.
Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as "Under the Sun." The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.
What technology is under consideration in the first project in this scenario?

A. Server driven controls.

B. Cloud computing
C. Data on demand
D. MAC filtering

Answer: A

NEW QUESTION 140
......