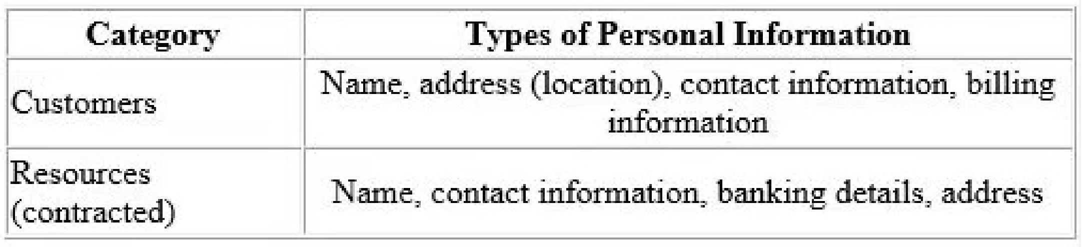
IAPP

Exam Questions CIPT

Certified Information Privacy Technologist

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
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
What IT architecture would be most appropriate for this mobile platform?

A. Peer-to-peer architecture.
B. Client-server architecture.
C. Plug-in-based architecture.
D. Service-oriented architecture.

Answer: D

NEW QUESTION 3
What is an example of a just-in-time notice?

A. A warning that a website may be unsafe.
B. A full organizational privacy notice publicly available on a website
C. A credit card company calling a user to verify a purchase before itis authorized
D. Privacy information given to a user when he attempts to comment on an online article.

Answer: D

NEW QUESTION 4
What is the main function of the Amnesic Incognito Live System or TAILS device?

A. It allows the user to run a self-contained computer from a USB device.
B. It accesses systems with a credential that leaves no discernable tracks.
C. It encrypts data stored on any computer on a network.
D. It causes a system to suspend its security protocols.

Answer: A

NEW QUESTION 5
When should code audits be concluded?

A. At code check-in time.
B. At engineering design time.
C. While code is being sent to production.
D. Before launch after all code for a feature is complete.

Answer: D

NEW QUESTION 6
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 7
What is the main function of a breach response center?

A. Detecting internal security attacks.
B. Addressing privacy incidents.
C. Providing training to internal constituencies.
D. Interfacing with privacy regulators and governmental bodies.

Answer: B

NEW QUESTION 8
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 9
Between November 30th and December 2nd, 2013, cybercriminals successfully infected the credit card payment systems and bypassed security controls of a United States-based retailer with malware that exfiltrated 40 million credit card numbers. Six months prior, the retailer had malware detection software installed to prevent against such an attack.
Which of the following would best explain why the retailer’s consumer data was still exfiltrated?

A. The detection software alerted the retailer’s security operations center per protocol, but the information security personnel failed to act upon the alerts.
B. The U.S Department of Justice informed the retailer of the security breach on De
C. 12th, but the retailer took three days to confirm the breach and eradicate the malware.
D. The IT systems and security measures utilized by the retailer’s third-party vendors were in compliance with industry standards, but their credentials were stolen by black hat hackers who then entered the retailer’s system.
E. The retailer’s network that transferred personal data and customer payments was separate from the rest of the corporate network, but the malware code was disguised with the name of software that is supposed to protect this information.

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

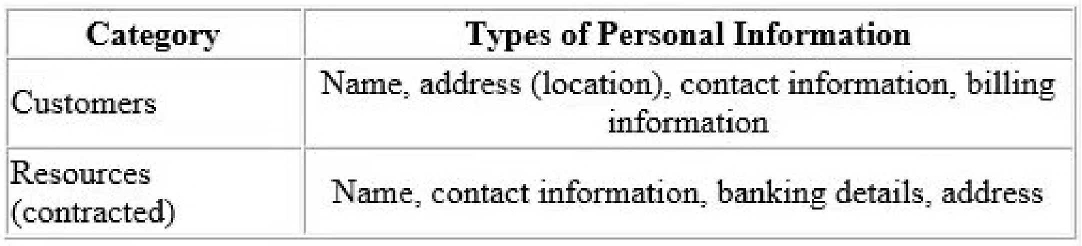
NEW QUESTION 10
SCENARIO
Please use the following to answer the next question:
Light Blue Health (LBH) is a healthcare technology company developing a new web and mobile application that collects personal health information from electronic patient health records. The application will use machine learning to recommend potential medical treatments and medications based on information collected from anonymized electronic health records. Patient users may also share health data collected from other mobile apps with the LBH app.
The application requires consent from the patient before importing electronic health records into the application and sharing it with their authorized physicians or healthcare provider. The patient can then review and share the recommended treatments with their physicians securely through the app. The patient user may also share location data and upload photos in the app. The patient user may also share location data and upload photos in the app for a healthcare provider to review along with the health record. The patient may also delegate access to the app.
LBH’s privacy team meets with the Application development and Security teams, as well as key business stakeholders on a periodic basis. LBH also implements Privacy by Design (PbD) into the application development process.
The Privacy Team is conducting a Privacy Impact Assessment (PIA) to evaluate privacy risks during development of the application. The team must assess

whether the application is collecting descriptive, demographic or any other user related data from the electronic health records that are not needed for the purposes of the application. The team is also reviewing whether the application may collect additional personal data for purposes for which the user did not provide consent.
What is the best way to ensure that the application only collects personal data that is needed to fulfill its primary purpose of providing potential medical and healthcare recommendations?

A. Obtain consent before using personal health information for data analytics purposes.
B. Provide the user with an option to select which personal data the application may collect.
C. Disclose what personal data the application the collecting in the company Privacy Policy posted online.
D. Document each personal category collected by the app and ensure it maps to an app function or feature.

Answer: C

NEW QUESTION 11
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.

Considering that LeadOps will host/process personal information on behalf of Clean-Q remotely, what is an appropriate next step for Clean-Q senior management to assess LeadOps' appropriateness?

A. Nothing at this stage as the Managing Director has made a decision.
B. Determine if any Clean-Q competitors currently use LeadOps as a solution.
C. Obtain a legal opinion from an external law firm on contracts management.
D. Involve the Information Security team to understand in more detail the types of services and solutions LeadOps is proposing.

Answer: D

NEW QUESTION 14
In order to prevent others from identifying an individual within a data set, privacy engineers use a cryptographically-secure hashing algorithm. Use of hashes in this way illustrates the privacy tactic known as what?

A. Isolation.
B. Obfuscation.
C. Perturbation.
D. Stripping.

Answer: B

NEW QUESTION 16
Which of the following is considered a records management best practice?

A. Archiving expired data records and files.
B. Storing decryption keys with their associated backup systems.
C. Implementing consistent handling practices across all record types.
D. Using classification to determine access rules and retention policy.

Answer: D

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 regulation most likely applies to the data stored by Berry Country Regional Medical Center?

A. Personal Information Protection and Electronic Documents Act
B. Health Insurance Portability and Accountability Act
C. The Health Records Act 2001
D. The European Union Directive 95/46/EC

Answer: A

NEW QUESTION 18
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.
Which should be used to allow the home sales force to accept payments using smartphones?

A. Field transfer protocol.
B. Cross-current translation.
C. Near-field communication
D. Radio Frequency Identification

Answer: C

NEW QUESTION 22
SCENARIO
Wesley Energy has finally made its move, acquiring the venerable oil and gas exploration firm Lancelot from its long-time owner David Wilson. As a member of the transition team, you have come to realize that Wilson's quirky nature affected even Lancelot's data practices, which are maddeningly inconsistent. “The old man hired and fired IT people like he was changing his necktie,” one of Wilson’s seasoned lieutenants tells you, as you identify the traces of initiatives left half complete.
For instance, while some proprietary data and personal information on clients and employees is encrypted, other sensitive information, including health information from surveillance testing of employees for toxic exposures, remains unencrypted, particularly when included within longer records with less-sensitive data. You also find that data is scattered across applications, servers and facilities in a manner that at first glance seems almost random.
Among your preliminary findings of the condition of data at Lancelot are the following:
- Cloud technology is supplied by vendors around the world, including firms that you have not heard of.

You are told by a former Lancelot employee that these vendors operate with divergent security requirements and protocols.
- The company’s proprietary recovery process for shale oil is stored on servers among a variety of less-sensitive information that can be accessed not only by scientists, but by personnel of all types at most company locations.
- DES is the strongest encryption algorithm currently used for any file.
- Several company facilities lack physical security controls, beyond visitor check-in, which familiar vendors often bypass.
- Fixing all of this will take work, but first you need to grasp the scope of the mess and formulate a plan of action to address it.

Which is true regarding the type of encryption Lancelot uses?

A. It employs the data scrambling technique known as obfuscation.
B. Its decryption key is derived from its encryption key.
C. It uses a single key for encryption and decryption.
D. It is a data masking methodology.

Answer: A

NEW QUESTION 25
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 30
SCENARIO
Please use the following to answer the next question:
Light Blue Health (LBH) is a healthcare technology company developing a new web and mobile application that collects personal health information from electronic patient health records. The application will use machine learning to recommend potential medical treatments and medications based on information collected from anonymized electronic health records. Patient users may also share health data collected from other mobile apps with the LBH app.
The application requires consent from the patient before importing electronic health records into the application and sharing it with their authorized physicians or healthcare provider. The patient can then review and share the recommended treatments with their physicians securely through the app. The patient user may also share location data and upload photos in the app. The patient user may also share location data and upload photos in the app for a healthcare provider to review along with the health record. The patient may also delegate access to the app.
LBH’s privacy team meets with the Application development and Security teams, as well as key business stakeholders on a periodic basis. LBH also implements Privacy by Design (PbD) into the application development process.
The Privacy Team is conducting a Privacy Impact Assessment (PIA) to evaluate privacy risks during development of the application. The team must assess whether the application is collecting descriptive, demographic or any other user related data from the electronic health records that are not needed for the purposes of the application. The team is also reviewing whether the application may collect additional personal data for purposes for which the user did not provide consent.
Regarding the app, which action is an example of a decisional interference violation?

A. The app asks income level to determine the treatment of care.
B. The app sells aggregated data to an advertising company without prior consent.
C. The app has a pop-up ad requesting sign-up for a pharmaceutical company newsletter.
D. The app asks questions during account set-up to disclose family medical history that is not necessary for the treatment of the individual’s symptoms.

Answer: D

NEW QUESTION 35
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 38
Not updating software for a system that processes human resources data with the latest security patches may create what?

A. Authentication issues.
B. Privacy vulnerabilities.
C. Privacy threat vectors.
D. Reportable privacy violations.

Answer: B

NEW QUESTION 40
During a transport layer security (TLS) session, what happens immediately after the web browser creates a random PreMasterSecret?

A. The server decrypts the PremasterSecret.
B. The web browser opens a TLS connection to the PremasterSecret.
C. The web browser encrypts the PremasterSecret with the server's public key.
D. The server and client use the same algorithm to convert the PremasterSecret into an encryption key.

Answer: C

NEW QUESTION 45
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 50
How should the sharing of information within an organization be documented?

A. With a binding contract.
B. With a data flow diagram.
C. With a disclosure statement.
D. With a memorandum of agreement.

Answer: C

NEW QUESTION 54
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 56
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 58
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 63
Which technique is most likely to facilitate the deletion of every instance of data associated with a deleted user account from every data store held by an organization?

A. Auditing the code which deletes user accounts.
B. Building a standardized and documented retention program for user data deletion.
C. Monitoring each data store for presence of data associated with the deleted user account.
D. Training engineering teams on the importance of deleting user accounts their associated data from all data stores when requested.

Answer: C

NEW QUESTION 68
Revocation and reissuing of compromised credentials is impossible for which of the following authentication techniques?

A. Biometric data.
B. Picture passwords.
C. Personal identification number.
D. Radio frequency identification.

Answer: D

NEW QUESTION 71
An EU marketing company is planning to make use of personal data captured to make automated decisions based on profiling. In some cases, processing and automated decisions may have a legal effect on individuals, such as credit worthiness.
When evaluating the implementation of systems making automated decisions, in which situation would the company have to accommodate an individual's right NOT to be subject to such processing to ensure compliance under the General Data Protection Regulation (GDPR)?

A. When an individual’s legal status or rights are not affected by the decision.
B. When there is no human intervention or influence in the decision-making process.
C. When the individual has given explicit consent to such processing and suitable safeguards exist.
D. When the decision is necessary for entering into a contract and the individual can contest the decision.

Answer: B

NEW QUESTION 72
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 77
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."

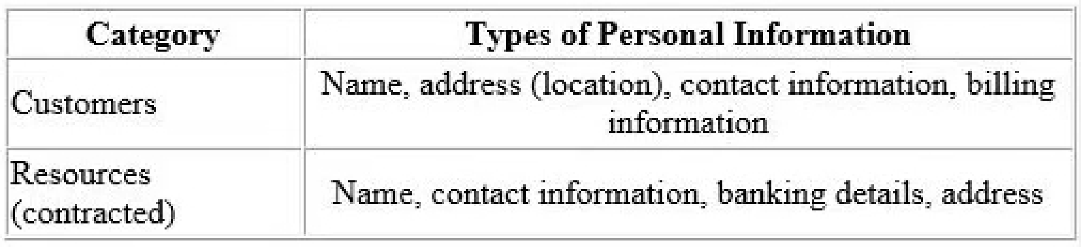
Answer: A

NEW QUESTION 78
What is the term for information provided to a social network by a member?

A. Profile data.
B. Declared data.
C. Personal choice data.
D. Identifier information.

Answer: A

NEW QUESTION 82
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.

What is a key consideration for assessing external service providers like LeadOps, which will conduct personal information processing operations on Clean-Q's behalf?

A. Understanding LeadOps’ costing model.
B. Establishing a relationship with the Managing Director of LeadOps.
C. Recognizing the value of LeadOps’ website holding a verified security certificate.
D. Obtaining knowledge of LeadOps' information handling practices and information security environment.

Answer: D

NEW QUESTION 87
SCENARIO
Carol was a U.S.-based glassmaker who sold her work at art festivals. She kept things simple by only accepting cash and personal checks.
As business grew, Carol couldn't keep up with demand, and traveling to festivals became burdensome. Carol opened a small boutique and hired Sam to run it

while she worked in the studio. Sam was a natural salesperson, and business doubled. Carol told Sam, “I don't know what you are doing, but keep doing it!"
But months later, the gift shop was in chaos. Carol realized that Sam needed help so she hired Jane, who had business expertise and could handle the back-office tasks. Sam would continue to focus on sales. Carol gave Jane a few weeks to get acquainted with the artisan craft business, and then scheduled a meeting for the three of them to discuss Jane's first impressions.
At the meeting, Carol could not wait to hear Jane's thoughts, but she was unprepared for what Jane had to say. “Carol, I know that he doesn't realize it, but some of Sam’s efforts to increase sales have put you in a vulnerable position. You are not protecting customers’ personal information like you should.”
Sam said, “I am protecting our information. I keep it in the safe with our bank deposit. It's only a list of
customers’ names, addresses and phone numbers that I get from their checks before I deposit them. I contact them when you finish a piece that I think they would like. That's the only information I have! The only other thing I do is post photos and information about your work on the photo sharing site that I use with family and friends. I provide my email address and people send me their information if they want to see more of your work. Posting online really helps sales, Carol. In fact, the only complaint I hear is about having to come into the shop to make a purchase.”
Carol replied, “Jane, that doesn’t sound so bad. Could you just fix things and help us to post even more online?"
‘I can," said Jane. “But it's not quite that simple. I need to set up a new program to make sure that we follow the best practices in data management. And I am concerned for our customers. They should be able to manage how we use their personal information. We also should develop a social media strategy.”
Sam and Jane worked hard during the following year. One of the decisions they made was to contract with an outside vendor to manage online sales. At the end of the year, Carol shared some exciting news. “Sam and Jane, you have done such a great job that one of the biggest names in the glass business wants to buy us out! And Jane, they want to talk to you about merging all of our customer and vendor information with theirs beforehand."
Which regulator has jurisdiction over the shop's data management practices?

A. The Federal Trade Commission.
B. The Department of Commerce.
C. The Data Protection Authority.
D. The Federal Communications Commission.

Answer: A

NEW QUESTION 92
A company seeking to hire engineers in Silicon Valley ran an ad campaign targeting women in a specific age range who live in the San Francisco Bay Area. Which Calo objective privacy harm is likely to result from this campaign?

A. Lost opportunity.
B. Economic loss.
C. Loss of liberty.
D. Social detriment.

Answer: D

NEW QUESTION 94
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 99
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.
What is the most secure method Finley Motors should use to transmit Chuck’s information to AMP Payment Resources?

A. Cloud file transfer services.
B. Certificate Authority (CA).
C. HyperText Transfer Protocol (HTTP).
D. Transport Layer Security (TLS).

Answer: D

NEW QUESTION 104
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: C

NEW QUESTION 108
Which of the following statements describes an acceptable disclosure practice?

A. An organization's privacy policy discloses how data will be used among groups within the organization itself.
B. With regard to limitation of use, internal disclosure policies override contractual agreements with third parties.
C. Intermediaries processing sensitive data on behalf of an organization require stricter disclosure oversight than vendors.
D. When an organization discloses data to a vendor, the terms of the vendor' privacy notice prevail over the organization' privacy notice.

Answer: A

NEW QUESTION 109
What is the most important requirement to fulfill when transferring data out of an organization?

A. Ensuring the organization sending the data controls how the data is tagged by the receiver.
B. Ensuring the organization receiving the data performs a privacy impact assessment.
C. Ensuring the commitments made to the data owner are followed.
D. Extending the data retention schedule as needed.

Answer: C

NEW QUESTION 112
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
What would be the best way to supervise the third-party systems the EnsureClaim App will share data with?

A. Review the privacy notices for each third-party that the app will share personal data with to determine adequate privacy and data protection controls are in place.
B. Conduct a security and privacy review before onboarding new vendors that collect personal data from the app.
C. Anonymize all personal data collected by the app before sharing any data with third-parties.
D. Develop policies and procedures that outline how data is shared with third-party apps.

Answer: C

NEW QUESTION 115
Aadhaar is a unique-identity number of 12 digits issued to all Indian residents based on their biometric and demographic data. The data is collected by the Unique Identification Authority of India. The Aadhaar database contains the Aadhaar number, name, date of birth, gender and address of over 1 billion individuals.
Which of the following datasets derived from that data would be considered the most de-identified?

A. A count of the years of birth and hash of the person' s gender.
B. A count of the month of birth and hash of the person's first name.
C. A count of the day of birth and hash of the person's first initial of their first name.
D. Account of the century of birth and hash of the last 3 digits of the person's Aadhaar number.

Answer: C

NEW QUESTION 116
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 118
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 119
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 120
A company configures their information system to have the following capabilities: Allow for selective disclosure of attributes to certain parties, but not to others.
Permit the sharing of attribute references instead of attribute values - such as “I am over 21” instead of birthday date.
Allow for information to be altered or deleted as needed.
These capabilities help to achieve which privacy engineering objective?

A. Predictability.
B. Manageability.
C. Disassociability.
D. Integrity.

Answer: C

NEW QUESTION 125
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.
Why is Jordan’s claim that the company does not collect personal information as identified by the GDPR inaccurate?

A. The potential customers must browse for products online.
B. The fitness trackers capture sleep and heart rate data to monitor an individual’s behavior.
C. The website collects the customers’ and users’ region and country information.
D. The customers must pair their fitness trackers to either smartphones or computers.

Answer: A

NEW QUESTION 129
Which of the following does NOT illustrate the ‘respect to user privacy’ principle?

A. Implementing privacy elements within the user interface that facilitate the use of technology by any visually-challenged users.
B. Enabling Data Subject Access Request (DSARs) that provide rights for correction, deletion, amendment and rectification of personal information.
C. Developing a consent management self-service portal that enables the data subjects to review the details of consent provided to an organization.
D. Filing breach notification paperwork with data protection authorities which detail the impact to data subjects.

Answer: D

NEW QUESTION 134
SCENARIO
Tom looked forward to starting his new position with a U.S —based automobile leasing company (New Company), now operating in 32 states. New Company was recently formed through the merger of two prominent players, one from the eastern region (East Company) and one from the western region (West Company). Tom, a Certified Information Privacy Technologist (CIPT), is New Company's first Information Privacy and Security Officer. He met today with Dick from East Company, and Harry, from West Company. Dick and Harry are veteran senior information privacy and security professionals at their respective companies, and continue to lead the east and west divisions of New Company. The purpose of the meeting was to conduct a SWOT (strengths/weaknesses/opportunities/threats)

analysis for New Company. Their SWOT analysis conclusions are summarized below.
Dick was enthusiastic about an opportunity for the New Company to reduce costs and increase computing power and flexibility through cloud services. East Company had been contemplating moving to the cloud, but West Company already had a vendor that was providing it with software-as-a-service (SaaS). Dick was looking forward to extending this service to the eastern region. Harry noted that this was a threat as well, because West Company had to rely on the third party to protect its data.
Tom mentioned that neither of the legacy companies had sufficient data storage space to meet the projected growth of New Company, which he saw as a weakness. Tom stated that one of the team's first projects would be to construct a consolidated New Company data warehouse. Tom would personally lead this project and would be held accountable if information was modified during transmission to or during storage in the new data warehouse.
Tom, Dick and Harry agreed that employee network access could be considered both a strength and a weakness. East Company and West Company had strong performance records in this regard; both had robust network access controls that were working as designed. However, during a projected year-long transition period, New Company employees would need to be able to connect to a New Company network while retaining access to the East Company and West Company networks.
When employees are working remotely, they usually connect to a Wi-Fi network. What should Harry advise for maintaining company security in this situation?

A. Hiding wireless service set identifiers (SSID).
B. Retaining the password assigned by the network.
C. Employing Wired Equivalent Privacy (WEP) encryption.
D. Using tokens sent through HTTP sites to verify user identity.

Answer: A

NEW QUESTION 136
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 138
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.
Ted's implementation is most likely a response to what incident?

A. Encryption keys were previously unavailable to the organization's cloud storage host.
B. Signatureless advanced malware was detected at multiple points on the organization's networks.
C. Cyber criminals accessed proprietary data by running automated authentication attacks on the organization's network.
D. Confidential information discussed during a strategic teleconference was intercepted by the organization's top competitor.

Answer: A

NEW QUESTION 143
Which is NOT a suitable method for assuring the quality of data collected by a third-party company?

A. Verifying the accuracy of the data by contacting users.

B. Validating the company’s data collection procedures.
C. Introducing erroneous data to see if its detected.
D. Tracking changes to data through auditing.

Answer: A

NEW QUESTION 148
......