Number: CIPT
Passing Score: 800
Time Limit: 120
File Version: 13.0

Exam Code: CIPT
Exam Name: Certified Information Privacy Technologist (CIPT)

Exam A

QUESTION 1
Which of the following are the mandatory pieces of information to be included in the documentation of records of processing activities for an organization that processes personal data on behalf of another organization?

A. Copies of the consent forms from each data subject.
B. Time limits for erasure of different categories of data.
C. Contact details of the processor and Data Protection Offer (DPO).
D. Descriptions of the processing activities and relevant data subjects.

Correct Answer: B
Section:

QUESTION 2
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.

Correct Answer: A
Section:

QUESTION 3
Which of the following is the best method to minimize tracking through the use of cookies?

A. Use 'private browsing' mode and delete checked files, clear cookies and cache once a day.
B. Install a commercially available third-party application on top of the browser that is already installed.
C. Install and use a web browser that is advertised as 'built specifically to safeguard user privacy'.
D. Manage settings in the browser to limit the use of cookies and remove them once the session completes.

Correct Answer: D
Section:

QUESTION 4
Which of the following is NOT relevant to a user exercising their data portability rights?

A. Notice and consent for the downloading of data.
B. Detection of phishing attacks against the portability interface.

C. Re-authentication of an account, including two-factor authentication as appropriate.
D. Validation of users with unauthenticated identifiers (e.g. IP address, physical address).

Correct Answer: D
Section:

QUESTION 5
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.

Correct Answer: B
Section:

QUESTION 6
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.

Correct Answer: C
Section:

QUESTION 7
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.

Correct Answer: C
Section:
Explanation:
The Data Protection Authority is a regulatory body responsible for enforcing data protection laws and ensuring that organizations comply with their obligations to protect personal data. The Federal Trade Commission (FTC) is an independent agency of the United States government whose primary mission is to promote consumer protection and prevent anti-competitive business practices.

QUESTION 8
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."
When initially collecting personal information from customers, what should Jane be guided by?

A. Onward transfer rules.
B. Digital rights management.
C. Data minimization principles.
D. Vendor management principles

Correct Answer: C
Section:
Explanation:
When initially collecting personal information from customers, Jane should be guided by data minimization principles ©. Data minimization involves collecting only the minimum amount of personal data necessary to achieve a specific purpose. This means that Jane should only collect personal information from customers that is relevant and necessary for the intended purpose and should avoid collecting excessive or unnecessary data.

QUESTION 9
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.

Correct Answer: C
Section:
Explanation:
A key principle of an effective privacy policy is that it should be presented with external parties as the intended audience1. This means that the privacy policy should be clear, easily understandable, and accessible to anyone who interacts with the organization or its services. The privacy policy should also inform external parties about how their personal data is collected, processed, stored, shared, and protected by the organization2. The other options are not principles of an effective privacy policy, but rather potential pitfalls or limitations.

QUESTION 10
What was the first privacy framework to be developed?

A. OECD Privacy Principles.
B. Generally Accepted Privacy Principles.
C. Code of Fair Information Practice Principles (FIPPs).
D. The Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

Correct Answer: C
Section:
Explanation:
The first privacy framework to be developed was the Code of Fair Information Practice Principles (FIPPs)3. The FIPPs were proposed by a US government advisory committee in 1973 as a set of guidelines for protecting personal data in automated systems3. The FIPPs influenced many subsequent privacy frameworks and laws around the world, such as the OECD Privacy Principles (1980), the EU Data Protection Directive (1995), and the APEC Privacy Framework (2004)3.

QUESTION 11
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.

Correct Answer: D
Section:
Explanation:
Reference: https://privacyrights.org/resources/review-fair-information-principles-foundation-privacy-public-policy The Organization for Economic Co-operation and Development (OECD) Privacy Principles became a foundation for privacy principles and practices of countries and organizations across the globe4. The OECD Privacy Principles were adopted by OECD member countries in 1980 as a set of eight basic principles for ensuring adequate protection of personal data across national borders4. The OECD Privacy Principles have been widely recognized as an international standard for data protection and have influenced many regional and national laws and frameworks4.

QUESTION 12
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.

Correct Answer: C
Section:
Explanation:
In the scenario, Ted implemented a new security measure that requires all employees to use twofactor authentication when accessing the organization's network. This measure is most likely a response to an incident where cyber criminals accessed proprietary data by running automated authentication attacks on the organization's network.

QUESTION 13
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.

Correct Answer: C
Section:
Explanation:
Jill is leading an initiative to develop a new industry standard for data privacy and security. Kyle should recommend that Jill seek support from industry groups as they are likely to have a vested interest in the development of such a standard and may be able to provide valuable input and resources.

QUESTION 14
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

Correct Answer: A
Section:
Explanation:
Barney is leading a project to improve the organization's data practices and has implemented a new policy that requires all employees to delete any data that is no longer needed for business purposes.
This suggests that Barney is most likely focused on improving the organization's data deletion practices.

QUESTION 15
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.

Correct Answer: B
Section:
Explanation:
The main function of a breach response center is to address privacy incidents1. A breach response center is a team of experts that conducts a comprehensive breach response when a data breach occurs1. The breach response center may include forensics, legal, information security, information technology, operations, human resources, communications, investor relations, and management1.
The other options are not the main function of a breach response center, but rather possible tasks or roles that may be involved in a breach response.

QUESTION 16
Which is NOT a suitable action to apply to data when the retention period ends?

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

Correct Answer: D
Section:
Explanation:
Retagging is not a suitable action to apply to data when the retention period ends2. Retagging means changing the classification or label of data based on its sensitivity or value2. Retagging does not reduce the risk of unauthorized access or disclosure of personal data that is no longer needed by the organization2. The other options are suitable actions to apply to data when the retention period ends, as they either remove or anonymize personal data2.

QUESTION 17

What is the distinguishing feature of asymmetric encryption?

A. It has a stronger key for encryption than for decryption.
B. It employs layered encryption using dissimilar methods.
C. It uses distinct keys for encryption and decryption.
D. It is designed to cross operating systems.

Correct Answer: C
Section:
Explanation:
Reference: https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties
The distinguishing feature of asymmetric encryption is that it uses distinct keys for encryption and decryption3. Asymmetric encryption, also known as public-key encryption, involves two keys: a public key that can be shared with anyone and used to encrypt messages; and a private key that is kept secret by its owner and used to decrypt messages3. The other options are not features of asymmetric encryption.

QUESTION 18
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.

Correct Answer: C
Section:
Explanation:
The most important requirement to fulfill when transferring data out of an organization is ensuring the commitments made to the data owner are followed. The data owner is the person who has provided their personal data to an organization for a specific purpose or consented to its collection.
When transferring data out of an organization, such as sharing it with another entity or moving it across borders, it is essential that the organization respects the rights and expectations of the data owner and complies with any applicable laws or regulations. The other options are not requirements for transferring data out of an organization, but rather possible measures or considerations that may be relevant depending on the context or nature of the transfer.

QUESTION 19
Which activity would best support the principle of data quality?

A. Providing notice to the data subject regarding any change in the purpose for collecting such data.
B. Ensuring that the number of teams processing personal information is limited.
C. Delivering information in a format that the data subject understands.
D. Ensuring that information remains accurate.

Correct Answer: D
Section:
Explanation:
Reference: https://iapp.org/resources/article/fair-information-practices/
The principle of data quality states that personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and up to date1. Therefore, ensuring that information remains accurate is an activity that would best support this principle1. The other options are not directly related to the principle of data quality, but rather to other principles such as purpose specification, security safeguards, or openness.

QUESTION 20

Which Organization for Economic Co-operation and Development (OECD) privacy protection principle encourages an organization to obtain an individual s consent before transferring personal information?

A. Individual participation.
B. Purpose specification.
C. Collection limitation.
D. Accountability.

Correct Answer: A
Section:
Explanation:
The individual participation principle encourages an organization to obtain an individual's consent before transferring personal information1. According to this principle, an individual should have the right to obtain from a data controller confirmation of whether or not the data controller has data relating to him; to have communicated to him such data within a reasonable time; to be given reasons if a request made under subparagraphs (a) and (b) is denied by the data controller; and to challenge such denial; and to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended1. The other options are not principles that encourage an organization to obtain an individual's consent before transferring personal information. http://www.oecdprivacy.org/

QUESTION 21
Granting data subjects the right to have data corrected, amended, or deleted describes?

A. Use limitation.
B. Accountability.
C. A security safeguard
D. Individual participation

Correct Answer: D
Section:
Explanation:
Reference: https://www.ncbi.nlm.nih.gov/books/NBK236546/
Granting data subjects the right to have data corrected, amended, or deleted describes individual participation1. As explained above, the individual participation principle gives individuals certain rights over their personal data held by a data controller1. One of these rights is to challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed or amended1. The other options are not principles that describe granting data subjects this right.

QUESTION 22
What is a mistake organizations make when establishing privacy settings during the development of applications?

A. Providing a user with too many choices.
B. Failing to use "Do Not Track" technology.
C. Providing a user with too much third-party information.
D. Failing to get explicit consent from a user on the use of cookies.

Correct Answer: D
Section:
Explanation:
Failing to get explicit consent from a user on the use of cookies is a mistake organizations make when establishing privacy settings during the development of applications2. Cookies are small files that store information about users' preferences and behavior on websites2. They can be used for various purposes such as authentication, personalization, analytics, advertising etc.2 However, they can also pose privacy risks as they may collect sensitive or personal information without users' knowledge or consent2. Therefore, organizations should inform users about how they use cookies and obtain their explicit consent before placing cookies on their devices2. This is also required by some laws such as EU's General Data Protection Regulation (GDPR) and ePrivacy Directive2. The other options are not mistakes organizations make when establishing privacy settings during the development of applications.

QUESTION 23
Which of the following suggests the greatest degree of transparency?

A. A privacy disclosure statement clearly articulates general purposes for collection
B. The data subject has multiple opportunities to opt-out after collection has occurred.
C. A privacy notice accommodates broadly defined future collections for new products.
D. After reading the privacy notice, a data subject confidently infers how her information will be used.

Correct Answer: D
Section:
Explanation:
After reading the privacy notice, a data subject confidently infers how her information will be used suggests the greatest degree of transparency3
https://www.informatica.com/resources/articles/what-is-data-quality.html

QUESTION 24
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.

Correct Answer: C
Section:
Explanation:
Introducing erroneous data to see if it's detected is not a suitable method for assuring the quality of data collected by a third-party company1. This method could compromise the integrity and reliability of the data and cause confusion or harm to the users or the business1. The other options are suitable methods for assuring the quality of data collected by a third-party company1. Verifying the accuracy of the data by contacting users can help identify and correct any errors or inconsistencies in the data1. Validating the company's data collection procedures can help ensure that they follow best practices and standards for collecting, storing, and processing personal information1. Tracking changes to data through auditing can help monitor and document any modifications or deletions made to the data1.
https://www.isaca.org/resources/news-and-trends/industry-news/2021/data-minimization-apractical-approach

QUESTION 25
A valid argument against data minimization is that it?

A. Can limit business opportunities.
B. Decreases the speed of data transfers.
C. Can have an adverse effect on data quality.
D. Increases the chance that someone can be identified from data.

Correct Answer: A
Section:
Explanation:
A valid argument against data minimization is that it can limit business opportunities23. Data minimization refers to limiting the collection, storage, and processing of personal information to only what is strictly necessary for business operations3. While this practice can help protect privacy and security, it can also restrict the potential uses and benefits of data for innovation, research, marketing, analytics etc.23. The other options are not valid arguments against data minimization, but rather arguments in favor of it23.
https://www.manageengine.com/data-security/what-is/data-minimization.html

QUESTION 26

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.

Correct Answer: A
Section:

QUESTION 27
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.

Correct Answer: D
Section:

QUESTION 28
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."

Correct Answer: A
Section:
Explanation:
Reference: https://www.researchgate.net/publication/284332229_k-nonymity_A_Model_for_Protecting_Privacy

QUESTION 29
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.

Correct Answer: A
Section:

QUESTION 30
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.

Correct Answer: C
Section:

QUESTION 31
What can be used to determine the type of data in storage without exposing its contents?

A. Collection records.
B. Data mapping.
C. Server logs.
D. Metadata.

Correct Answer: D
Section:
Explanation:
Reference: https://cloud.google.com/storage/docs/gsutil/addlhelp/WorkingWithObjectMetadata

QUESTION 32
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.

Correct Answer: C
Section:

QUESTION 33
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.

Correct Answer: C
Section:

QUESTION 34
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.

Correct Answer: D
Section:
Explanation:
Reference: https://www.archive-vault.co.uk/best-practice-for-records-management

QUESTION 35
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.

Correct Answer: A
Section:

QUESTION 36
What tactic does pharming use to achieve its goal?

A. It modifies the user's Hosts file.
B. It encrypts files on a user's computer.
C. It creates a false display advertisement.
D. It generates a malicious instant message.

Correct Answer: C
Section:
Explanation:
Reference: https://inspiredelearning.com/blog/phishing-vs-pharming-whats-difference/

QUESTION 37
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.

Correct Answer: B
Section:

QUESTION 38
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.

Correct Answer: B
Section:
Explanation:
Reference: https://neilpatel.com/blog/behavioral-advertising/

QUESTION 39
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.

Correct Answer: C
Section:
Explanation:
Reference: https://en.wikipedia.org/wiki/Do_Not_Track

QUESTION 40
Why is first-party web tracking very difficult to prevent?

A. The available tools to block tracking would break most sites' functionality.
B. Consumers enjoy the many benefits they receive from targeted advertising.
C. Regulatory frameworks are not concerned with web tracking.
D. Most browsers do not support automatic blocking.

Correct Answer: D
Section:
Explanation:
Reference: https://www.opentracker.net/article/third-party-cookies-vs-first-party-cookies

QUESTION 41
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.

Correct Answer: C
Section:

Explanation:
Reference:
https://books.google.com.pk/books?id=OaXise4Bp8C&pg=PA175&lpg=PA175&dq=iapp+During+a+transport+layer+security+(TLS)+session,+what+happens+immediately+after+the+web+browser+creates+a+random+PreMasterSecret&source=bl&ots=zR0RCfnx3c&sig=ACfU3U0bTOeOfPfcoq_Y95SZs6imKKilug&hl=en&sa=X&ved=2ahUKEwjkscDHpcbnAhUJuRoKHU5iC9cQ6AEwCnoECAkQAQ#v=onepage&q=iapp%20During%20a%20transport%20layer%20security%20(TLS)%20session%2C%20what%20happens%20immediately%20after%20the%20web%20browser%20creates%20a%20random%20PreMasterSecret&f=false

QUESTION 42
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.

Correct Answer: C
Section:

QUESTION 43
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.

Correct Answer: C
Section:
Explanation:
The most important aspect to cover when advising on privacy concerns regarding paid advertisements would be C. Personal information collected by cookies linked to the advertising network. Cookies are small text files that are stored on a user's device by websites and advertising networks. They can be used to track a user's browsing behavior and collect personal information.
This can raise privacy concerns as users may not be aware of the extent of data collection and how their personal information is being used.

QUESTION 44

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

Correct Answer: B
Section:
Explanation:
The technology under consideration in the first project in this scenario is B. Cloud computing. In the scenario, it is mentioned that the first project involves migrating data and applications to a cloudbased infrastructure.

QUESTION 45
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

Correct Answer: C
Section:
Explanation:
The technology that should be used to allow the home sales force to accept payments using smartphones is C. Near-field communication (NFC). NFC is a short-range wireless technology that allows devices to exchange data when they are brought close together. This technology is commonly used in contactless payment systems and can be used to enable smartphones to accept payments.

QUESTION 46
What is the best way to protect privacy on a geographic information system (GIS)?

A. Limiting the data provided to the system.
B. Using a wireless encryption protocol.
C. Scrambling location information.
D. Using a firewall.

Correct Answer: A
Section:
Explanation:
Reference:
https://www.researchgate.net/publication/2873114_Protecting_Personal_Privacy_in_Using_Geographic_Information_Systems

QUESTION 47
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.

Correct Answer: B
Section:
Explanation:
Reference: https://towardsdatascience.com/notes-on-artificial-intelligence-ai-machine-learning-mland-deep-learning-dl-for-56e51a2071c2

QUESTION 48
Which of the following is an example of the privacy risks associated with the Internet of Things (IoT)?

A. A group of hackers infiltrate a power grid and cause a major blackout.
B. An insurance company raises a person's rates based on driving habits gathered from a connected car.
C. A website stores a cookie on a user's hard drive so the website can recognize the user on subsequent visits.
D. A water district fines an individual after a meter reading reveals excess water use during drought conditions.

Correct Answer: B
Section:

QUESTION 49

How can a hacker gain control of a smartphone to perform remote audio and video surveillance?

A. By performing cross-site scripting.
B. By installing a roving bug on the phone.
C. By manipulating geographic information systems.
D. By accessing a phone's global positioning system satellite signal.

Correct Answer: B
Section:

QUESTION 50
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.
If Clean-Q were to utilize LeadOps' services, what is a contract clause that may be included in the agreement entered into with LeadOps?

A. A provision that holds LeadOps liable for a data breach involving Clean-Q's information.
B. A provision prescribing technical and organizational controls that LeadOps must implement.
C. A provision that requires LeadOps to notify Clean-Q of any suspected breaches of information that involves customer or resource information managed on behalf of Clean-Q.
D. A provision that allows Clean-Q to conduct audits of LeadOps' information processing and information security environment, at LeadOps' cost and at any time that Clean-Q requires.

Correct Answer: D
Section:

QUESTION 51

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.

Correct Answer: D
Section:
Explanation:
Since LeadOps will host/process personal information on behalf of Clean-Q remotely, it is important for Clean-Q's Information Security team to assess the security measures and controls that LeadOps has in place to protect this information.
This will help Clean-Q senior management make an informed decision about whether or not to engage LeadOps' services.

QUESTION 52
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?

Correct Answer: C
Section:
Explanation:
The location of LeadOps' operations and hosting services is important information for Clean-Q to consider when assessing LeadOps' appropriateness as a service provider. This is because different countries have different data protection laws and regulations that may impact how personal information can be processed and stored. Knowing where LeadOps' operations and hosting services are located will help Clean-Q make informed decisions about how to protect the personal information it entrusts to LeadOps.

QUESTION 53
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.

Correct Answer: D
Section:
Explanation:
When engaging an external service provider to process personal information on its behalf, it is important for Clean-Q to have a good understanding of the service provider's information handling practices and information security environment. This will help Clean-Q assess whether or not the service provider has appropriate measures in place to protect the personal information it entrusts to them.

QUESTION 54
Which of the following is NOT a workplace surveillance best practice?

A. Check local privacy laws before putting surveillance in place.
B. Ensure surveillance is discreet so employees do not alter their behavior.
C. Once surveillance data has been gathered, limit exposure of the content.
D. Ensure the minimal amount of surveillance is performed to meet the objective.

Correct Answer: B
Section:

QUESTION 55
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.

Correct Answer: C
Section:

QUESTION 56
Which is the most accurate type of biometrics?

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

Correct Answer: B
Section:
Explanation:
Reference: https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/

QUESTION 57
What is true of providers of wireless technology?

A. They have the legal right in most countries to control and use any data on their systems.
B. They can see all unencrypted data that crosses the system.
C. They are typically exempt from data security regulations.
D. They routinely backup data that crosses their system.

Correct Answer: B
Section:

QUESTION 58
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.

Correct Answer: D
Section:
Explanation:
Reference: https://towardsdatascience.com/what-is-a-smart-device-the-key-concept-of-theinternet-of-things-52da69f6f91b

QUESTION 59
What is the goal of privacy enhancing technologies (PETS) like multiparty computation and differential privacy?

A. To facilitate audits of third party vendors.
B. To protect sensitive data while maintaining its utility.
C. To standardize privacy activities across organizational groups.
D. To protect the security perimeter and the data items themselves.

Correct Answer: B
Section:
Explanation:
Reference: https://royalsociety.org/-/media/policy/projects/privacy-enhancingtechnologies/privacy-report-summary.pdf

QUESTION 60
To comply with the Sarbanes-Oxley Act (SOX), public companies in the United States are required to annually report on the effectiveness of the auditing controls of their financial reporting systems. These controls must be implemented to prevent unauthorized use, disclosure, modification, and damage or loss of financial data.
Why do these controls ensure both the privacy and security of data?

A. Modification of data is an aspect of privacy; unauthorized use, disclosure, and damage or loss of data are aspects of security.
B. Unauthorized use of data is an aspect of privacy; disclosure, modification, and damage or loss of data are aspects of security.
C. Disclosure of data is an aspect of privacy; unauthorized use, modification, and damage or loss of data are aspects of security.
D. Damage or loss of data are aspects of privacy; disclosure, unauthorized use, and modification of data are aspects of privacy.

Correct Answer: C
Section:

QUESTION 61
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.

Correct Answer: C
Section:

QUESTION 62
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.

Correct Answer: D
Section:
Explanation:
Transferring personal data across borders can pose significant privacy risks if not done in compliance with applicable data protection laws and regulations. It is important for WebTracker to confirm that this data transfer has been fully approved by all relevant parties to ensure that it is being done in a compliant manner.

QUESTION 63
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.

Correct Answer: B
Section:
Explanation:
Sending marketing communications such as newsletters to customers involves processing their personal data. It is important for WebTracker's CPO to investigate whether this processing is being done in compliance with applicable data protection laws and regulations. This may include verifying that customers have given their consent to receive these communications or that another lawful basis for processing their personal data exists.

QUESTION 64
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-asa- 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.
Which statement is correct about addressing New Company stakeholders' expectations for privacy?

A. New Company should expect consumers to read the company's privacy policy.
B. New Company should manage stakeholder expectations for privacy even when the stakeholders' data is not held by New Company.
C. New Company would best meet consumer expectations for privacy by adhering to legal requirements.
D. New Company's commitment to stakeholders ends when the stakeholders' data leaves New Company.

Correct Answer: C
Section:
Explanation:
Adhering to legal requirements for data protection and privacy is an important way for New Company to meet its stakeholders' expectations for privacy. This includes complying with applicable data protection laws and regulations and implementing appropriate measures to protect personal data.

QUESTION 65
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.

Correct Answer: A
Section:
Explanation:
Instead, Harry should advise employees to use strong passwords or other forms of secure authentication such as multi-factor authentication when connecting to Wi-Fi networks. He should also advise them to use secure methods of encryption such as WPA2 or WPA3 when transmitting sensitive company data over Wi-Fi.

QUESTION 66
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

Correct Answer: A
Section:
Explanation:
Berry Country Regional Medical Center is located in Ontario, Canada. PIPEDA is a Canadian federal law that sets out rules for how private sector organizations must handle personal information in the course of commercial activities. Since Berry Country Regional Medical Center is a private sector organization that handles personal information in the course of its commercial activities, it would be subject to PIPEDA.

QUESTION 67
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.

Correct Answer: D
Section:

QUESTION 68
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.

Correct Answer: C
Section:

QUESTION 69
SCENARIO
Looking back at your first two years as the Director of Personal Information Protection and Compliance for the St. Anne's 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 recall a recent visit to the Records Storage Section in the basement of the old hospital next to the modern facility, where you noticed paper records sitting in crates labeled by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. On the back shelves of the section sat data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the records storage section, you noticed a man leaving whom you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.
You quickly realize that you need a plan of action on the maintenance, secure storage and disposal of data.
Which cryptographic standard would be most appropriate for protecting patient credit card information in the records system at St. Anne's Regional Medical Center?

A. Symmetric Encryption
B. Tokenization
C. Obfuscation
D. Certificates

Correct Answer: B
Section:

QUESTION 70
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.

Correct Answer: B
Section:

QUESTION 71
Which of these actions is NOT generally part of the responsibility of an IT or software engineer?

A. Providing feedback on privacy policies.
B. Implementing multi-factor authentication.
C. Certifying compliance with security and privacy law.
D. Building privacy controls into the organization's IT systems or software.

Correct Answer: A

Section:

QUESTION 72
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.

Correct Answer: C
Section:

QUESTION 73
Which of the following CANNOT be effectively determined during a code audit?

A. Whether access control logic is recommended in all cases.
B. Whether data is being incorrectly shared with a third-party.
C. Whether consent is durably recorded in the case of a server crash.
D. Whether the differential privacy implementation correctly anonymizes data.

Correct Answer: D
Section:

QUESTION 74
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.

Correct Answer: B
Section:

QUESTION 75
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.

Correct Answer: C
Section:
Explanation:
D. Obtain consent and capture geolocation data at all times after consent is received.
Answer: C
Explanation:
By providing users with a clear and explicit explanation about why geolocation data is needed and how it will be used, the app can help ensure that only the minimum amount of data necessary is collected. This can also help build trust with users and increase transparency.

QUESTION 76
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.

Correct Answer: B

Section:

QUESTION 77
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.

Correct Answer: D
Section:

QUESTION 78
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.

Correct Answer: B
Section:
Explanation:
Conducting a security and privacy review before onboarding new vendors can help EnsureClaim assess whether these vendors have appropriate measures in place to protect personal data. This can include reviewing their privacy policies and practices as well as their technical security controls.

QUESTION 79
What is the main privacy threat posed by Radio Frequency Identification (RFID)?

A. An individual with an RFID receiver can track people or consumer products.
B. An individual can scramble computer transmissions in weapons systems.
C. An individual can use an RFID receiver to engage in video surveillance.
D. An individual can tap mobile phone communications.

Correct Answer: D
Section:

QUESTION 80
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 should Finley Motors have done to incorporate the transparency principle of Privacy by Design (PbD)?

A. Signed a data sharing agreement with AMP Payment Resources.
B. Documented that Finley Motors has a legitimate interest to share Chuck's information.
C. Obtained verbal consent from Chuck and recorded it within internal systems.
D. Provided notice of data sharing practices within the electronically signed rental agreement.

Correct Answer: D
Section:
Explanation:
By providing clear and concise notice of its data sharing practices within the rental agreement that Chuck electronically signed, Finley Motors could have ensured that Chuck was informed about how his personal information would be used and shared. This would have helped to increase transparency and build trust with Chuck.

QUESTION 81

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).

Correct Answer: D
Section:
Explanation:
TLS is a cryptographic protocol that provides secure communication over a network. It can help protect against eavesdropping and tampering by encrypting data in transit. Cloud file transfer services (option A) can also provide secure transmission of data but their security depends on the specific service used. Certificate Authority (CA) (option B) is not a method for transmitting data but rather a trusted third party that issues digital certificates used for authentication.
HyperText Transfer Protocol (HTTP) (option C) is not a secure method for transmitting sensitive data as it does not provide encryption.

QUESTION 82
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.

Correct Answer: A
Section:

Explanation:
To reduce the risk associated with transferring Chuck's personal information to AMP Payment Resources, Finley Motors could take several steps. One such step would be option A: By providing only the minimum necessary data to process the violation notice and masking all other information prior to transfer.
By providing only the minimum necessary data to process the violation notice and masking all other information prior to transfer, Finley Motors can help reduce the risk associated with transferring Chuck's personal information. This can help ensure that only necessary data is shared and that any unnecessary or sensitive data is protected.

QUESTION 83
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 strongest method for authenticating Chuck's identity prior to allowing access to his violation information through the AMP Payment Resources web portal?

A. By requiring Chuck use the last 4 digits of his driver's license number in combination with a unique PIN provided within the violation notice.
B. By requiring Chuck use his credit card number in combination with the last 4 digits of his driver's license.
C. By requiring Chuck use the rental agreement number in combination with his email address.
D. By requiring Chuck to call AMP Payment Resources directly and provide his date of birth and home address.

Correct Answer: A
Section:
Explanation:
The strongest method for authenticating Chuck's identity prior to allowing access to his violation information through the AMP Payment Resources web portal would be option A: By requiring Chuck use the last 4 digits of his driver's license number in combination with a unique PIN provided within the violation notice.

QUESTION 84
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.

Correct Answer: C
Section:

QUESTION 85
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.

Correct Answer: B
Section:
Explanation:
Sleep and heart rate data collected by the fitness trackers can be considered personal information under the GDPR because it relates to an identified or identifiable natural person. This means that even if the company does not collect other types of personal information such as name or address, it is still collecting personal information as defined by the GDPR.

QUESTION 86
Which of the following is one of the fundamental principles of information security?

A. Accountability.
B. Accessibility.
C. Confidentiality.
D. Connectivity.

Correct Answer: C
Section:

QUESTION 87
An organization's customers have suffered a number of data breaches through successful social engineering attacks. One potential solution to remediate and prevent future occurrences would be to implement which of the following?

A. Differential identifiability.
B. Multi-factor authentication.
C. Greater password complexity.
D. Attribute-based access control.

Correct Answer: B
Section:
Explanation:
Multi-factor authentication. Social engineering attacks often involve tricking individuals into revealing their login credentials. Implementing multi-factor authentication can help prevent unauthorized access even if an attacker obtains a user's password.

QUESTION 88
An organization is launching a new online subscription-based publication. As the service is not aimed at children, users are asked for their date of birth as part of the of the sign-up process. The privacy technologist suggests it

may be more appropriate ask if an individual is over 18 rather than requiring they provide a date of birth. What kind of threat is the privacy technologist concerned about?

A. Identification.
B. Insecurity.
C. Interference.
D. Minimization.

Correct Answer: D
Section:
Explanation:
By suggesting that it may be more appropriate to ask if an individual is over 18 rather than requiring they provide a date of birth, the privacy technologist is concerned about minimizing the amount of personal data collected. This helps reduce privacy risks by limiting the amount of personal data that could potentially be exposed in a data breach.

QUESTION 89
Combining multiple pieces of information about an individual to produce a whole that is greater than the sum of its parts is called?

A. Identification.
B. Insecurity.
C. Aggregation.
D. Exclusion.

Correct Answer: C
Section:

QUESTION 90
A clinical research organization is processing highly sensitive personal data, including numerical attributes, from medical trial results. The organization needs to manipulate the data without revealing the contents to data users. This can be achieved by utilizing?

A. k-anonymity.
B. Microdata sets.
C. Polymorphic encryption.
D. Homomorphic encryption.

Correct Answer: D
Section:
Explanation:
Homomorphic encryption. Homomorphic encryption allows computations to be performed on encrypted data without revealing the contents of the data. This can be useful in situations where sensitive personal data needs to be processed without revealing its contents to data users.

QUESTION 91
To meet data protection and privacy legal requirements that may require personal data to be disposed of or deleted when no longer necessary for the use it was collected, what is the best privacy-enhancing solution a privacy technologist should recommend be implemented in application design to meet this requirement?

A. Implement a process to delete personal data on demand and maintain records on deletion requests.
B. Implement automated deletion of off-site backup of personal data based on annual risk assessments.
C. Develop application logic to validate and purge personal data according to legal hold status or retention schedule.
D. Securely archive personal data not accessed or used in the last 6 months. Automate a quarterly review to delete data from archive once no longer needed.

Correct Answer: A
Section:

QUESTION 92
An organization is reliant on temporary contractors for performing data analytics and they require access to personal data via software-as-a-service to perform their job. When the temporary contractor completes their work assignment, what woul^.be the most effective way to safeguard privacy and access to personal data when they leave?

A. Set a system-based expiry that requires management reauthorization for online access for accounts that have been active more than 6 months.
B. Establish a predetermined automatic account expiration date based on contract timescales.
C. Require temporary contractors to sign a non-disclosure agreement, security acceptable use policy, and online access authorizations by hiring managers.
D. Mandate hiring managers to email IT or Security team when the contractor leaves.

Correct Answer: B
Section:

QUESTION 93
Which of the following is a privacy consideration for NOT sending large-scale SPAM type emails to a database of email addresses?

A. Poor user experience.
B. Emails are unsolicited.
C. Data breach notification.
D. Reduction in email deliverability score.

Correct Answer: B
Section:

QUESTION 94
Which of the following can be used to bypass even the best physical and logical security mechanisms to gain access to a system?

A. Phishing emails.
B. Denial of service.
C. Brute-force attacks.
D. Social engineering.

Correct Answer: D
Section:

QUESTION 95
An organization is deciding between building a solution in-house versus purchasing a solution for a new customer facing application. When security threat are taken into consideration, a key advantage of purchasing a solution would be the availability of?

A. Outsourcing.
B. Persistent VPN.
C. Patching and updates.
D. Digital Rights Management.

Correct Answer: C

Section:

QUESTION 96
An organization is concerned that its aging IT infrastructure will lead to Increased security and privacy risks. Which of the following would help mitigate these risks?

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

Correct Answer: A
Section:

QUESTION 97
An organization has recently experienced a data breach where large amounts of personal data were compromised. As part of a post-incident review, the privacy technologist wants to analyze available data to understand what vulnerabilities may have contributed to the incident occurring. He learns that a key vulnerability had been flagged by the system but that detective controls were not operating effectively. Which type of web application security risk does this finding most likely point to?

A. Insecure Design.
B. Misconfiguration.
C. Vulnerable and Outdated Components.
D. Logging and Monitoring Failures.

Correct Answer: D
Section:

QUESTION 98
Data oriented strategies Include which of the following?

A. Minimize. Separate, Abstract, Hide.
B. Inform, Control, Enforce, Demonstrate.
C. Encryption, Hashing, Obfuscation, Randomization.
D. Consent. Contract, Legal Obligation, Legitimate interests.

Correct Answer: A
Section:

QUESTION 99
There are two groups of users. In a company, where one group Is allowed to see credit card numbers, while the other group Is not. Both are accessing the data through the same application. The most effective and efficient way to achieve this would be?

A. Have two copies of the data, one copy where the credit card numbers are obfuscated, while the other copy has them in the clear. Serve up from the appropriate copy depending on the user accessing it.
B. Have the data encrypted at rest, and selectively decrypt It for the users who have the rights to see it.
C. Obfuscate the credit card numbers whenever a user who does not have the right to see them accesses the data.
D. Drop credit card numbers altogether whenever a user who does not have the right to see them accesses the data.

Correct Answer: B

Section:

QUESTION 100
Which of the following is NOT a valid basis for data retention?

A. Size of the data.
B. Type of the data.
C. Location of the data.
D. Last time the data was accessed.

Correct Answer: D
Section:

QUESTION 101
Which of the following techniques describes the use of encryption where encryption keys are divided into parts that can then be used to recover a full encryption key?

A. Homomorphic encryption.
B. Asymmetric cryptography.
C. Cryptographic hashing.
D. Secret sharing.

Correct Answer: D
Section:

QUESTION 102
SCENARIO
Please use the following to answer the next questions:
Your company is launching a new track and trace health app during the outbreak of a virus pandemic in the US. The developers claim the app is based on privacy by design because personal data collected was considered to ensure only necessary data is captured, users are presented with a privacy notice, and they are asked to give consent before data is shared. Users can update their consent after logging into an account, through a dedicated privacy and consent hub.
This is accessible through the 'Settings' icon from any app page, then clicking 'My Preferences', and selecting 'Information Sharing and Consent' where the following choices are displayed:
• "I consent to receive notifications and infection alerts";
• "I consent to receive information on additional features or services, and new products";
• "I consent to sharing only my risk result and location information, for exposure and contact tracing purposes";
• "I consent to share my data for medical research purposes"; and
• "I consent to share my data with healthcare providers affiliated to the company".
For each choice, an ON* or OFF tab is available The default setting is ON for all Users purchase a virus screening service for USS29 99 for themselves or others using the app The virus screening service works as follows:
• Step 1 A photo of the user's face is taken.
• Step 2 The user measures their temperature and adds the reading in the app
• Step 3 The user is asked to read sentences so that a voice analysis can detect symptoms
• Step 4 The user is asked to answer questions on known symptoms
• Step 5 The user can input information on family members (name date of birth, citizenship, home address, phone number, email and relationship).) The results are displayed as one of the following risk status "Low. "Medium" or "High" if the user is deemed at "Medium " or "High" risk an alert may be sent to other users and the user is Invited to seek a medical consultation and diagnostic from a healthcare provider.
A user's risk status also feeds a world map for contact tracing purposes, where users are able to check if they have been or are in dose proximity of an infected person If a user has come in contact with another individual classified as "medium' or 'high' risk an instant notification also alerts the user of this. The app collects location trails of every user to monitor locations visited by an infected individual Location is collected using the phone's GPS functionary, whether the app is in use or not however, the exact location of the user is "blurred' for privacy reasons Users can only see on the map circles What is likely to be the biggest privacy concern with the current 'Information Sharing and Consent' page?

A. The ON or OFF default setting for each item.
B. The navigation needed in the app to get to the consent page.
C. The option to consent to receive potential marketing information.
D. The information sharing with healthcare providers affiliated with the company.

Correct Answer: A
Section:
Explanation:
Having default settings for information sharing and consent can be problematic because it may not accurately reflect a user's preferences. Users may not be aware of these default settings or may not understand their implications. This could result in personal information being shared without the user's explicit consent.

QUESTION 103
SCENARIO
Please use the following to answer the next questions:
Your company is launching a new track and trace health app during the outbreak of a virus pandemic in the US. The developers claim the app is based on privacy by design because personal data collected was considered to ensure only necessary data is captured, users are presented with a privacy notice, and they are asked to give consent before data is shared. Users can update their consent after logging into an account, through a dedicated privacy and consent hub.
This is accessible through the 'Settings' icon from any app page, then clicking 'My Preferences', and selecting 'Information Sharing and Consent' where the following choices are displayed:
• "I consent to receive notifications and infection alerts";
• "I consent to receive information on additional features or services, and new products";
• "I consent to sharing only my risk result and location information, for exposure and contact tracing purposes";
• "I consent to share my data for medical research purposes"; and
• "I consent to share my data with healthcare providers affiliated to the company".
For each choice, an ON* or OFF tab is available The default setting is ON for all Users purchase a virus screening service for US$29 99 for themselves or others using the app The virus screening service works as follows:
• Step 1 A photo of the user's face is taken.
• Step 2 The user measures their temperature and adds the reading in the app
• Step 3 The user is asked to read sentences so that a voice analysis can detect symptoms
• Step 4 The user is asked to answer questions on known symptoms
• Step 5 The user can input information on family members (name date of birth, citizenship, home address, phone number, email and relationship).)
The results are displayed as one of the following risk status "Low. "Medium" or "High" if the user is deemed at "Medium " or "High" risk an alert may be sent to other users and the user is Invited to seek a medical consultation and diagnostic from a healthcare provider.
A user's risk status also feeds a world map for contact tracing purposes, where users are able to check if they have been or are in dose proximity of an infected person If a user has come in contact with another individual classified as "medium' or 'high' risk an instant notification also alerts the user of this. The app collects location trails of every user to monitor locations visited by an infected individual Location is collected using the phone's GPS functionary, whether the app is in use or not however, the exact location of the user is "blurred' for privacy reasons Users can only see on the map circles Which of the following is likely to be the most important issue with the choices presented in the 'Information
Sharing and Consent' pages?

A. The data and recipients for medical research are not specified
B. Insufficient information is provided on notifications and infection alerts
C. The sharing of information with an affiliated healthcare provider is too risky
D. Allowing users to share risk result information for exposure and contact tracing purposes

Correct Answer: A
Section:
Explanation:
Not specifying the data and recipients for medical research can make it difficult for users to make informed decisions about whether to consent to this type of information sharing. This lack of transparency could result in personal information being shared with third parties without the user's full understanding or consent.

QUESTION 104

SCENARIO
Please use the following to answer the next questions:
Your company is launching a new track and trace health app during the outbreak of a virus pandemic in the US. The developers claim the app is based on privacy by design because personal data collected was considered to ensure only necessary data is captured, users are presented with a privacy notice, and they are asked to give consent before data is shared. Users can update their consent after logging into an account, through a dedicated privacy and consent hub.
This is accessible through the 'Settings' icon from any app page, then clicking 'My Preferences', and selecting 'Information Sharing and Consent' where the following choices are displayed:
• "I consent to receive notifications and infection alerts";
• "I consent to receive information on additional features or services, and new products";
• "I consent to sharing only my risk result and location information, for exposure and contact tracing purposes";
• "I consent to share my data for medical research purposes"; and
• "I consent to share my data with healthcare providers affiliated to the company".
For each choice, an ON* or OFF tab is available The default setting is ON for all Users purchase a virus screening service for USS29 99 for themselves or others using the app The virus screening service works as follows:
• Step 1 A photo of the user's face is taken.
• Step 2 The user measures their temperature and adds the reading in the app
• Step 3 The user is asked to read sentences so that a voice analysis can detect symptoms
• Step 4 The user is asked to answer questions on known symptoms
• Step 5 The user can input information on family members (name date of birth, citizenship, home address, phone number, email and relationship).) The results are displayed as one of the following risk status "Low. "Medium" or "High" if the user is deemed at "Medium " or "High" risk an alert may be sent to other users and the user is Invited to seek a medical consultation and diagnostic from a healthcare provider.
A user's risk status also feeds a world map for contact tracing purposes, where users are able to check if they have been or are in dose proximity of an infected person If a user has come in contact with another individual classified as "medium' or 'high' risk an instant notification also alerts the user of this. The app collects location trails of every user to monitor locations visited by an infected individual Location is collected using the phone's GPS functionary, whether the app is in use or not however, the exact location of the user is "blurred' for privacy reasons Users can only see on the map circles Which of the following pieces of information collected is the LEAST likely to be justified tor the purposes of the app?

A. Relationship of family member
B. Phone number
C. Dale of birth
D. Citizenship

Correct Answer: D
Section:
Explanation:
Of the pieces of information collected by the app described in the scenario provided in the exhibit you shared, citizenship (option D) is LEAST likely to be justified for the purposes of the app.
Citizenship may not be necessary for providing health recommendations or contact tracing services.
Collecting this type of personal information could raise privacy concerns if it is not necessary for fulfilling the primary purpose of the app.

QUESTION 105
SCENARIO
Please use the following to answer the next questions:
Your company is launching a new track and trace health app during the outbreak of a virus pandemic in the US. The developers claim the app is based on privacy by design because personal data collected was considered to ensure only necessary data is captured, users are presented with a privacy notice, and they are asked to give consent before data is shared. Users can update their consent after logging into an account, through a dedicated privacy and consent hub.
This is accessible through the 'Settings' icon from any app page, then clicking 'My Preferences', and selecting 'Information Sharing and Consent' where the following choices are displayed:
• "I consent to receive notifications and infection alerts";
• "I consent to receive information on additional features or services, and new products";
• "I consent to sharing only my risk result and location information, for exposure and contact tracing purposes";
• "I consent to share my data for medical research purposes"; and
• "I consent to share my data with healthcare providers affiliated to the company".
For each choice, an ON* or OFF tab is available The default setting is ON for all Users purchase a virus screening service for USS29 99 for themselves or others using the app The virus screening service works as follows:
• Step 1 A photo of the user's face is taken.

• Step 2 The user measures their temperature and adds the reading in the app
• Step 3 The user is asked to read sentences so that a voice analysis can detect symptoms
• Step 4 The user is asked to answer questions on known symptoms
• Step 5 The user can input information on family members (name date of birth, citizenship, home address, phone number, email and relationship).) The results are displayed as one of the following risk status "Low. "Medium" or "High" if the user is deemed at "Medium " or "High" risk an alert may be sent to other users and the user is Invited to seek a medical consultation and diagnostic from a healthcare provider.
A user's risk status also feeds a world map for contact tracing purposes, where users are able to check if they have been or are in dose proximity of an infected person If a user has come in contact with another individual classified as "medium' or 'high' risk an instant notification also alerts the user of this. The app collects location trails of every user to monitor locations visited by an infected individual Location is collected using the phone's GPS functionary, whether the app is in use or not however, the exact location of the user is "blurred' for privacy reasons Users can only see on the map circles The location data collected and displayed on the map should be changed for which of the following reasons?

A. The blurriness does not allow users to know how close they are to an infected person
B. The radius used for location data exceeds official social distancing rules
C. The location data has not been pseudonymized
D. The location data is loo precise

Correct Answer: D
Section:
Explanation:
Location data that is too precise can reveal sensitive information about an individual's movements and activities. This could raise privacy concerns if this detailed location data is shared with third parties or used for purposes other than contact tracing. Pseudonymizing location data (option C) could also help protect user privacy but may not address concerns about overly precise location data.

QUESTION 106
SCENARIO
Please use the following to answer the next questions:
Your company is launching a new track and trace health app during the outbreak of a virus pandemic in the US. The developers claim the app is based on privacy by design because personal data collected was considered to ensure only necessary data is captured, users are presented with a privacy notice, and they are asked to give consent before data is shared. Users can update their consent after logging into an account, through a dedicated privacy and consent hub.
This is accessible through the 'Settings' icon from any app page, then clicking 'My Preferences', and selecting 'Information Sharing and Consent' where the following choices are displayed:
• "I consent to receive notifications and infection alerts";
• "I consent to receive information on additional features or services, and new products";
• "I consent to sharing only my risk result and location information, for exposure and contact tracing purposes";
• "I consent to share my data for medical research purposes"; and
• "I consent to share my data with healthcare providers affiliated to the company".
For each choice, an ON* or OFF tab is available The default setting is ON for all Users purchase a virus screening service for USS29 99 for themselves or others using the app The virus screening service works as follows:
• Step 1 A photo of the user's face is taken.
• Step 2 The user measures their temperature and adds the reading in the app
• Step 3 The user is asked to read sentences so that a voice analysis can detect symptoms
• Step 4 The user is asked to answer questions on known symptoms
• Step 5 The user can input information on family members (name date of birth, citizenship, home address, phone number, email and relationship).) The results are displayed as one of the following risk status "Low. "Medium" or "High" if the user is deemed at "Medium " or "High" risk an alert may be sent to other users and the user is Invited to seek a medical consultation and diagnostic from a healthcare provider.
A user's risk status also feeds a world map for contact tracing purposes, where users are able to check if they have been or are in dose proximity of an infected person If a user has come in contact with another individual classified as "medium' or 'high' risk an instant notification also alerts the user of this. The app collects location trails of every user to monitor locations visited by an infected individual Location is collected using the phone's GPS functionary, whether the app is in use or not however, the exact location of the user is "blurred' for privacy reasons Users can only see on the map circles Which technology is best suited for the contact tracing feature of the app1?

A. Bluetooth
B. Deep learning
C. Near Field Communication (NFC)
D. Radio-Frequency Identification (RFID)

Correct Answer: A
Section:
Explanation:
Bluetooth technology can enable devices to communicate with each other over short distances. This makes it well-suited for contact tracing applications where proximity between individuals needs to be detected. Deep learning (option B), Near Field Communication (NFC) (option C), and Radio- Frequency Identification (RFID) (option D) are technologies that could also have potential uses in a contact tracing app but may not be as well-suited as Bluetooth.

QUESTION 107
An organization needs to be able to manipulate highly sensitive personal information without revealing the contents of the data to the users. The organization should investigate the use of?

A. Advanced Encryption Standard (AES)
B. Homomorphic encryption
C. Quantum encryption
D. Pseudonymization

Correct Answer: B
Section:

QUESTION 108
A healthcare provider would like to data mine information for research purposes however the Chief Privacy Officer is concerned medical data of individuals may be disclosed overcome the concern, which is the preferred technique for protecting such data while still allowing for analysis?

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

Correct Answer: D
Section:

QUESTION 109
A privacy technologist has been asked to aid in a forensic investigation on the darknet following the compromise of a company's personal dat a. This will primarily involve an understanding of which of the following privacy-preserving techniques?

A. Encryption
B. Do Not Track
C. Masking
D. Tokenization

Correct Answer: A
Section:

QUESTION 110
Which of these is considered an ethical dark pattern on privacy?

A. Using attractive designs to influence an individual.
B. Rewarding users for providing more personal information

C. Giving users more privacy options in relation to their personal information
D. Providing dear and simple privacy notices to users

Correct Answer: B
Section:

QUESTION 111
Which concept related to privacy choice is demonstrated by highlighting and bolding the "accept" button on a cookies notice while maintaining standard text format for other options?

A. Illuminating
B. Nudging
C. Suppression
D. Tagging

Correct Answer: B
Section:

QUESTION 112
Truncating the last octet of an IP address because it is NOT needed is an example of which privacy principle?

A. Use Limitation
B. Data Minimization
C. Purpose Limitation
D. Security Safeguards

Correct Answer: B
Section:
Explanation:
Data minimization is a privacy principle that involves collecting and processing only the minimum amount of personal data necessary for a specific purpose.

QUESTION 113
Which privacy engineering objective proposed by the US National Institute of Science and Technology (NIST) decreases privacy risk by ensuring that connections between individuals and their personal data are reduced?

A. Disassoc lability
B. Manageability
C. Minimization
D. Predictability

Correct Answer: A
Section:

QUESTION 114
What is the main privacy threat posed by Radio Frequency Identification (RFID)?

A. RFID can be utilized to track people or consumer products
B. RFID can be utilized to gam unauthorized access to an individual's device
C. RFID can be utilized to spoof identification details

D. RFID can be utilized to read information from a device without the user's knowledge

Correct Answer: A
Section:

QUESTION 115
A jurisdiction requiring an organization to place a link on the website that allows a consumer to optout of sharing is an example of what type of requirement?

A. Functional
B. Operational
C. Technical
D. Use case

Correct Answer: B
Section:

QUESTION 116
An organization is using new technologies that will target and process personal data of EU customers.
In which of the following circumstances would a privacy technologist need to support a data protection impact assessment (DPIA)?

A. If a privacy notice and opt-m consent box are not displayed to the individual
B. If security of data processing has not been evaluated
C. If a large amount of personal data will be collected.
D. If data processing is a high risk to an individual's rights and freedoms

Correct Answer: D
Section:

QUESTION 117
Which of the following activities would be considered the best method for an organization to achieve the privacy principle of data quality'?

A. Clash customer information with information from a data broker
B. Build a system with user access controls and approval workflows to edit customer data
C. Set a privacy notice covering the purpose for collection of a customer's data
D. Provide a customer with a copy of their data in a machine-readable format

Correct Answer: B
Section:

QUESTION 118
A developer is designing a new system that allows an organization's helpdesk to remotely connect into the device of the individual to provide support Which of the following will be a privacy technologist's primary concern"?

A. Geofencing
B. Geo-tracking
C. Geo-tagging
D. Geolocation

Correct Answer: D
Section:

QUESTION 119
What risk is mitigated when routing meeting video traffic through a company's application servers rather than sending the video traffic directly from one user to another?

A. The user's identity is protected from the other user
B. The user is protected against cyberstalking attacks
C. The user's IP address is hidden from the other user
D. The user is assured that stronger authentication methods have been used

Correct Answer: C
Section:

QUESTION 120
An organization is evaluating a number of Machine Learning (ML) solutions to help automate a customer-facing part of its business From a privacy perspective, the organization should first?

A. Define their goals for fairness
B. Document the distribution of bias scores
C. Document the False Positive Rates (FPR).
D. Define how data subjects may object to the processing

Correct Answer: D
Section:
Explanation:
This involves establishing clear and transparent mechanisms for individuals to exercise their rights with respect to their personal data.

QUESTION 121
How does browser fingerprinting compromise privacy?

A. By creating a security vulnerability.
B. By differentiating users based upon parameters.
C. By persuading users to provide personal information.
D. By customizing advertising based on the geographic location.

Correct Answer: B
Section:
Explanation:
Browser fingerprinting involves collecting information about a user's device and browser configuration in order to uniquely identify them. This can allow for tracking of user behavior across websites without their knowledge or consent.

QUESTION 122
A computer user navigates to a page on the Internet. The privacy notice pops up and the user clicks the box to accept cookies, then continues to scroll the page to read the Information displayed. This is an example of which type of consent?

A. Explicit.
B. Implicit.

C. Specific
D. Valid.

Correct Answer: C
Section:

QUESTION 123
Many modern vehicles incorporate technologies that increase the convenience of drivers, but collect information about driver behavior in order to Implement this. What should vehicle manufacturers prioritize to ensure enhanced privacy protection for drivers?

A. Share the sensitive data collected about driver behavior with the driver.
B. Derive implicit consent for the processing of sensitive data by the continued use of the vehicle.
C. Obtain affirmative consent for processing of sensitive data about the driver.
D. Provide easy to read, in-vehicle instructions about how to use the technology.

Correct Answer: C
Section:

QUESTION 124
An organization is launching a smart watch which, in addition to alerts, will notify the the wearer of incoming calls allowing them to answer on the device. This convenience also comes with privacy concerns and is an example of?

A. Value-Sensitive Design.
B. Ubiquitous computing.
C. Anthropomorphism.
D. Coupling

Correct Answer: B
Section:
Explanation:
An organization launching a smart watch which notifies wearers of incoming calls allowing them to answer on the device would be an example of ubiquitous computing rather than coupling.
Ubiquitous computing refers to technology that is seamlessly integrated into everyday life and allows for constant connectivity and interaction.

QUESTION 125
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

Correct Answer: A
Section:

QUESTION 126
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

Correct Answer: B
Section:
Explanation:
To protect patient credit card information in the records system at Berry Country Regional Medical Center, an appropriate cryptographic standard to use would be option B: Symmetric Encryption.
Symmetric encryption uses a single secret key to encrypt and decrypt data. It is a fast and efficient method of encryption that can provide strong protection for sensitive data such as credit card information when implemented correctly.

QUESTION 127
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.

Correct Answer: D
Section:

QUESTION 128
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 sounds. It runs on battery power and automatically connects to a base station at home to charge itself.
C. A math tutoring service commissioned an advertisement on a bulletin board inside a charter school. The service makes it simple to reach out to tutors through a QR-code shaped like a cartoon character.
D. A note-taking application converts hard copies of kids' class notes into audio books in seconds. It does so by using the processing power of idle server farms.

Correct Answer: A
Section:

QUESTION 129
What is the main issue pertaining to data protection with the use of 'deep fakes'?

A. Misinformation.
B. Non-conformity with the accuracy principle.
C. Issues with establishing non-repudiation.
D. Issues with confidentiality of the information.

Correct Answer: A
Section:

QUESTION 130
An organization is considering launching enhancements to improve security and authentication mechanisms in their products. To better identify the user and reduce friction from the authentication process, they plan to track physical attributes of an individual. A privacy technologist assessing privacy implications would be most interested in which of the following?

A. The purpose of the data tracking.
B. That the individual is aware tracking is occurring.
C. The authentication mechanism proposed.
D. The encryption of individual physical attributes.

Correct Answer: A
Section:

QUESTION 131
Which of the following best describes the basic concept of "Privacy by Design?"

A. The adoption of privacy enhancing technologies.
B. The integration of a privacy program with all lines of business.
C. The implementation of privacy protection through system architecture.
D. The introduction of business process to identify and assess privacy gaps.

Correct Answer: C
Section: