

Exam Questions CIPT

Certified Information Privacy Technologist

<https://www.2passeasy.com/dumps/CIPT/>



NEW QUESTION 1

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

- A. Pharming.
- B. SQL injection.
- C. Malware execution.
- D. System modification.

Answer: B

NEW QUESTION 2

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

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

Answer: A

NEW QUESTION 3

Which is NOT a drawback to using a biometric recognition system?

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

Answer: A

NEW QUESTION 4

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.

Answer: A

NEW QUESTION 5

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

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

Answer: C

NEW QUESTION 6

SCENARIO

Please use the following to answer the next question:

Light Blue Health (LBH) is a healthcare technology company developing a new web and mobile application that collects personal health information from electronic patient health records. The application will use machine learning to recommend potential medical treatments and medications based on information collected from anonymized electronic health records. Patient users may also share health data collected from other mobile apps with the LBH app.

The application requires consent from the patient before importing electronic health records into the application and sharing it with their authorized physicians or healthcare provider. The patient can then review and share the recommended treatments with their physicians securely through the app. The patient user may also share location data and upload photos in the app. The patient user may also share location data and upload photos in the app for a healthcare provider to review along with the health record. The patient may also delegate access to the app.

LBH's privacy team meets with the Application development and Security teams, as well as key business stakeholders on a periodic basis. LBH also implements Privacy by Design (PbD) into the application development process.

The Privacy Team is conducting a Privacy Impact Assessment (PIA) to evaluate privacy risks during development of the application. The team must assess whether the application is collecting descriptive, demographic or any other user related data from the electronic health records that are not needed for the purposes of the application. The team is also reviewing whether the application may collect additional personal data for purposes for which the user did not provide consent.

What is the best way to ensure that the application only collects personal data that is needed to fulfill its primary purpose of providing potential medical and healthcare recommendations?

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

Answer: C

NEW QUESTION 7

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.

Answer: B

NEW QUESTION 8

What has been found to undermine the public key infrastructure system?

- A. Man-in-the-middle attacks.
- B. Inability to track abandoned keys.
- C. Disreputable certificate authorities.
- D. Browsers missing a copy of the certificate authority's public key.

Answer: D

NEW QUESTION 9

SCENARIO

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

Which cryptographic standard would be most appropriate for protecting patient credit card information in the records system?

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

Answer: A

NEW QUESTION 10

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

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

Answer: B

NEW QUESTION 10

SCENARIO

Please use the following to answer the next question:

Chuck, a compliance auditor for a consulting firm focusing on healthcare clients, was required to travel to the client's office to perform an onsite review of the client's operations. He rented a car from Finley Motors upon arrival at the airport as so he could commute to and from the client's office. The car rental agreement was electronically signed by Chuck and included his name, address, driver's license, make/model of the car, billing rate, and additional details describing the rental transaction. On the second night, Chuck was caught by a red light camera not stopping at an intersection on his way to dinner. Chuck returned the car back to the car rental agency at the end week without mentioning the infraction and Finley Motors emailed a copy of the final receipt to the address on file.

Local law enforcement later reviewed the red light camera footage. As Finley Motors is the registered owner of the car, a notice was sent to them indicating the infraction and fine incurred. This notice included the license plate number, occurrence date and time, a photograph of the driver, and a web portal link to a video clip of the violation for further review. Finley Motors, however, was not responsible for the violation as they were not driving the car at the time and transferred the incident to AMP Payment Resources for further review. AMP Payment Resources identified Chuck as the driver based on the rental agreement he signed when picking up the car and then contacted Chuck directly through a written letter regarding the infraction to collect the fine.

After reviewing the incident through the AMP Payment Resources' web portal, Chuck paid the fine using his personal credit card. Two weeks later, Finley Motors sent Chuck an email promotion offering 10% off a future rental.

How can Finley Motors reduce the risk associated with transferring Chuck's personal information to AMP Payment Resources?

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

Answer: A

NEW QUESTION 12

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.

Answer: A

NEW QUESTION 17

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

Answer: D

NEW QUESTION 21

What is a main benefit of data aggregation?

- A. It is a good way to perform analysis without needing a statistician.
- B. It applies two or more layers of protection to a single data record.
- C. It allows one to draw valid conclusions from small data samples.
- D. It is a good way to achieve de-identification and unlinkability.

Answer: C

NEW QUESTION 25

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

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

Answer: C

NEW QUESTION 28

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.

Answer: C

NEW QUESTION 31

What is the potential advantage of homomorphic encryption?

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

Answer: C

NEW QUESTION 36

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

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

Answer: C

NEW QUESTION 41

What is an Access Control List?

- A. A list of steps necessary for an individual to access a resource.
- B. A list that indicates the type of permission granted to each individual.
- C. A list showing the resources that an individual has permission to access.
- D. A list of individuals who have had their access privileges to a resource revoked.

Answer: C

NEW QUESTION 44

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

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

Answer: B

NEW QUESTION 49

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

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

Answer: C

NEW QUESTION 54

SCENARIO

Please use the following to answer the next question:

Jordan just joined a fitness-tracker start-up based in California, USA, as its first Information Privacy and Security Officer. The company is quickly growing its business but does not sell any of the fitness trackers itself. Instead, it relies on a distribution network of third-party retailers in all major countries. Despite not having any stores, the company has a 78% market share in the EU. It has a website presenting the company and products, and a member section where customers can access their information. Only the email address and physical address need to be provided as part of the registration process in order to customize the site to the user's region and country. There is also a newsletter sent every month to all members featuring fitness tips, nutrition advice, product spotlights from partner companies based on user behavior and preferences.

Jordan says the General Data Protection Regulation (GDPR) does not apply to the company. He says the company is not established in the EU, nor does it have a processor in the region. Furthermore, it does not do any "offering goods or services" in the EU since it does not do any marketing there, nor sell to consumers directly. Jordan argues that it is the customers who chose to buy the products on their own initiative and there is no "offering" from the company.

The fitness trackers incorporate advanced features such as sleep tracking, GPS tracking, heart rate monitoring, wireless syncing, calorie-counting and step-tracking. The watch must be paired with either a smartphone or a computer in order to collect data on sleep levels, heart rates, etc. All information from the device must be sent to the company's servers in order to be processed, and then the results are sent to the smartphone or computer. Jordan argues that there is no personal information involved since the company does not collect banking or social security information.

Based on the current features of the fitness watch, what would you recommend be implemented into each device in order to most effectively ensure privacy?

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

Answer: C

NEW QUESTION 59

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.

Answer: C

NEW QUESTION 63

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

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

Answer: C

NEW QUESTION 65

SCENARIO

Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company's information security policy and industry standards. Kyle is also new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle's schedule included participating in meetings and observing work in the IT and compliance departments.

Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization's wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.

Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company's privacy risk assessment, noting that the secondary use of personal information was considered a high risk.

By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn't wait to recommend his friend Ben who would be perfect for the job.

Which data practice is Barney most likely focused on improving?

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

Answer: C

NEW QUESTION 66

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.

Answer: A

NEW QUESTION 68

Which of the following functionalities can meet some of the General Data Protection Regulation's (GDPR's) Data Portability requirements for a social networking app designed for users in the EU?

- A. Allow users to modify the data they provided the app.
- B. Allow users to delete the content they provided the app.
- C. Allow users to download the content they have provided the app.
- D. Allow users to get a time-stamped list of what they have provided the app.

Answer: C

NEW QUESTION 72

SCENARIO

Please use the following to answer next question:

EnsureClaim is developing a mobile app platform for managing data used for assessing car accident insurance claims. Individuals use the app to take pictures at the crash site, eliminating the need for a built-in vehicle camera. EnsureClaim uses a third-party hosting provider to store data collected by the app. EnsureClaim customer service employees also receive and review app data before sharing with insurance claim adjusters.

The app collects the following information: First and last name

Date of birth (DOB) Mailing address Email address

Car VIN number Car model License plate

Insurance card number Photo

Vehicle diagnostics Geolocation

The app is designed to collect and transmit geolocation data. How can data collection best be limited to the necessary minimum?

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

Answer: D

NEW QUESTION 73

An EU marketing company is planning to make use of personal data captured to make automated decisions based on profiling. In some cases, processing and automated decisions may have a legal effect on individuals, such as credit worthiness.

When evaluating the implementation of systems making automated decisions, in which situation would the company have to accommodate an individual's right NOT to be subject to such processing to ensure compliance under the General Data Protection Regulation (GDPR)?

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

Answer: B

NEW QUESTION 76

In day to day interactions with technology, consumers are presented with privacy choices. Which of the following best represents the Privacy by Design (PbD) methodology of letting the user choose a non-zero-sum choice?

- A. Using images, words, and contexts to elicit positive feelings that result in proactive behavior, thus eliminating negativity and biases.
- B. Providing plain-language design choices that elicit privacy-related responses, helping users avoid errors and minimize the negative consequences of errors when they do occur.
- C. Displaying the percentage of users that chose a particular option, thus enabling the user to choose the most preferred option.
- D. Using contexts, antecedent events, and other priming concepts to assist the user in making a better privacy choice.

Answer: B

NEW QUESTION 81

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

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

Answer: B

NEW QUESTION 83

What is the main benefit of using a private cloud?

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

Answer: C

NEW QUESTION 84

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

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

Answer: A

NEW QUESTION 86

SCENARIO

Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company's information security policy and industry standards. Kyle is also new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle's schedule included participating in meetings and observing work in the IT and compliance departments.

Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization's wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.

Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company's privacy risk assessment, noting that the secondary use of personal information was considered a high risk.

By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn't wait to recommend his friend Ben who would be perfect for the job.

Which of the following should Kyle recommend to Jill as the best source of support for her initiative?

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

Answer: C

NEW QUESTION 88

A user who owns a resource wants to give other individuals access to the resource. What control would apply?

- A. Mandatory access control.
- B. Role-based access controls.
- C. Discretionary access control.
- D. Context of authority controls.

Answer: B

NEW QUESTION 93

SCENARIO

It should be the most secure location housing data in all of Europe, if not the world. The Global Finance Data Collective (GFDC) stores financial information and other types of client data from large banks, insurance companies, multinational corporations and governmental agencies. After a long climb on a mountain road

that leads only to the facility, you arrive at the security booth. Your credentials are checked and checked again by the guard to visually verify that you are the person pictured on your passport and national identification card. You are led down a long corridor with server rooms on each side, secured by combination locks built into the doors. You climb a flight of stairs and are led into an office that is lighted brilliantly by skylights where the GFDC Director of Security, Dr. Monique Batch, greets you. On the far wall you notice a bank of video screens showing different rooms in the facility. At the far end, several screens show different sections of the road up the mountain

Dr. Batch explains once again your mission. As a data security auditor and consultant, it is a dream assignment: The GFDC does not want simply adequate controls, but the best and most effective security that current technologies allow.

"We were hacked twice last year," Dr. Batch says, "and although only a small number of records were stolen, the bad press impacted our business. Our clients count on us to provide security that is nothing short of impenetrable and to do so quietly. We hope to never make the news again." She notes that it is also essential that the facility is in compliance with all relevant security regulations and standards.

You have been asked to verify compliance as well as to evaluate all current security controls and security measures, including data encryption methods, authentication controls and the safest methods for transferring data into and out of the facility. As you prepare to begin your analysis, you find yourself considering an intriguing question: Can these people be sure that I am who I say I am?

You are shown to the office made available to you and are provided with system login information, including the name of the wireless network and a wireless key. Still pondering, you attempt to pull up the facility's wireless network, but no networks appear in the wireless list. When you search for the wireless network by name, however it is readily found.

Why would you recommend that GFC use record encryption rather than disk, file or table encryption?

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

Answer: B

NEW QUESTION 96

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

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

Answer: C

NEW QUESTION 98

SCENARIO

Carol was a U.S.-based glassmaker who sold her work at art festivals. She kept things simple by only accepting cash and personal checks.

As business grew, Carol couldn't keep up with demand, and traveling to festivals became burdensome. Carol opened a small boutique and hired Sam to run it while she worked in the studio. Sam was a natural salesperson, and business doubled. Carol told Sam, "I don't know what you are doing, but keep doing it!"

But months later, the gift shop was in chaos. Carol realized that Sam needed help so she hired Jane, who had business expertise and could handle the back-office tasks. Sam would continue to focus on sales. Carol gave Jane a few weeks to get acquainted with the artisan craft business, and then scheduled a meeting for the three of them to discuss Jane's first impressions.

At the meeting, Carol could not wait to hear Jane's thoughts, but she was unprepared for what Jane had to say. "Carol, I know that he doesn't realize it, but some of Sam's efforts to increase sales have put you in a vulnerable position. You are not protecting customers' personal information like you should."

Sam said, "I am protecting our information. I keep it in the safe with our bank deposit. It's only a list of

customers' names, addresses and phone numbers that I get from their checks before I deposit them. I contact them when you finish a piece that I think they would like. That's the only information I have! The only other thing I do is post photos and information about your work on the photo sharing site that I use with family and friends. I provide my email address and people send me their information if they want to see more of your work. Posting online really helps sales, Carol. In fact, the only complaint I hear is about having to come into the shop to make a purchase."

Carol replied, "Jane, that doesn't sound so bad. Could you just fix things and help us to post even more online?"

"I can," said Jane. "But it's not quite that simple. I need to set up a new program to make sure that we follow the best practices in data management. And I am concerned for our customers. They should be able to manage how we use their personal information. We also should develop a social media strategy."

Sam and Jane worked hard during the following year. One of the decisions they made was to contract with an outside vendor to manage online sales. At the end of the year, Carol shared some exciting news. "Sam and Jane, you have done such a great job that one of the biggest names in the glass business wants to buy us out! And Jane, they want to talk to you about merging all of our customer and vendor information with theirs beforehand."

Which regulator has jurisdiction over the shop's data management practices?

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

Answer: A

NEW QUESTION 103

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

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

Answer: B

NEW QUESTION 107

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

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

Answer: D

NEW QUESTION 111

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.

Answer: D

NEW QUESTION 114

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

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

Answer: C

NEW QUESTION 119

What logs should an application server retain in order to prevent phishing attacks while minimizing data retention?

- A. Limited-retention, de-identified logs including only metadata.
- B. Limited-retention, de-identified logs including the links clicked in messages as well as metadata.
- C. Limited-retention logs including the identity of parties sending and receiving messages as well as metadata.
- D. Limited-retention logs including the links clicked in messages, the identity of parties sending and receiving them, as well as metadata.

Answer: B

NEW QUESTION 120

SCENARIO

Please use the following to answer next question:

EnsureClaim is developing a mobile app platform for managing data used for assessing car accident insurance claims. Individuals use the app to take pictures at the crash site, eliminating the need for a built-in vehicle camera. EnsureClaim uses a third-party hosting provider to store data collected by the app. EnsureClaim customer service employees also receive and review app data before sharing with insurance claim adjusters.

The app collects the following information: First and last name

Date of birth (DOB) Mailing address Email address

Car VIN number Car model License plate

Insurance card number Photo

Vehicle diagnostics Geolocation

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

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

Answer: C

NEW QUESTION 122

Which of the following would be the best method of ensuring that Information Technology projects follow Privacy by Design (PbD) principles?

- A. Develop a technical privacy framework that integrates with the development lifecycle.
- B. Utilize Privacy Enhancing Technologies (PETs) as a part of product risk assessment and management.
- C. Identify the privacy requirements as a part of the Privacy Impact Assessment (PIA) process during development and evaluation stages.

D. Develop training programs that aid the developers in understanding how to turn privacy requirements into actionable code and design level specifications.

Answer: D

NEW QUESTION 123

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.

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.

Answer: D

NEW QUESTION 128

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.

Answer: D

NEW QUESTION 133

SCENARIO

Kyle is a new security compliance manager who will be responsible for coordinating and executing controls to ensure compliance with the company's information security policy and industry standards. Kyle is also new to the company, where collaboration is a core value. On his first day of new-hire orientation, Kyle's schedule included participating in meetings and observing work in the IT and compliance departments.

Kyle spent the morning in the IT department, where the CIO welcomed him and explained that her department was responsible for IT governance. The CIO and Kyle engaged in a conversation about the importance of identifying meaningful IT governance metrics. Following their conversation, the CIO introduced Kyle to Ted and Barney. Ted is implementing a plan to encrypt data at the transportation level of the organization's wireless network. Kyle would need to get up to speed on the project and suggest ways to monitor effectiveness once the implementation was complete. Barney explained that his short-term goals are to establish rules governing where data can be placed and to minimize the use of offline data storage.

Kyle spent the afternoon with Jill, a compliance specialist, and learned that she was exploring an initiative for a compliance program to follow self-regulatory privacy principles. Thanks to a recent internship, Kyle had some experience in this area and knew where Jill could find some support. Jill also shared results of the company's privacy risk assessment, noting that the secondary use of personal information was considered a high risk.

By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn't wait to recommend his friend Ben who would be perfect for the job.

Ted's implementation is most likely a response to what incident?

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

Answer: A

NEW QUESTION 135

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CIPT Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CIPT Product From:

<https://www.2passeasy.com/dumps/CIPT/>

Money Back Guarantee

CIPT Practice Exam Features:

- * CIPT Questions and Answers Updated Frequently
- * CIPT Practice Questions Verified by Expert Senior Certified Staff
- * CIPT Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CIPT Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year