Free Questions for CIPT by certscare

Shared by Beck on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

A- Restricting access to data based on location.

B- Restricting access to data based on user role.

C- Preventing certain types of devices from accessing data.

D- Preventing data from being placed in unprotected storage.

Answer:

B

Question 2

Question Type: MultipleChoice

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

Options:

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

Question 3

Question Type: MultipleChoice

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?

Options:

A- Hashing.

B- A2DP Bluetooth profile.

C- Persistent unique identifier.

D- Randomized MAC address.

Answer:

D

Explanation:

To most effectively ensure privacy in the fitness watch described in the scenario provided in the exhibit you shared, one feature that could be implemented into each device would be option D: Randomized MAC address.

Question 4

Question Type: **MultipleChoice**

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?

Options:

A- The potential customers must browse for products online.

B- The fitness trackers capture sleep and heart rate data to monitor an individual's behavior.

C- The website collects the customers' and users' region and country information.

D- The customers must pair their fitness trackers to either smartphones or computers.

Answer:

B

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 5

Question Type: MultipleChoice

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

Options:

A- Security systems can be used to enforce compliance with privacy policies.

B- Privacy and security are independent; organizations must decide which should by emphasized.

C- Privacy restricts access to personal information; security regulates how information should be used.

D- Privacy protects data from being viewed during collection and security governs how collected data should be shared.

Answer:

C

Question 6

Question Type: **MultipleChoice**

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?

Options:

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.

Answer:

A

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 7

Question Type: MultipleChoice

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?

Options:

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

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 8

Question Type: MultipleChoice

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?

Options:

A- Cloud file transfer services.

B- Certificate Authority (CA).

C- HyperText Transfer Protocol (HTTP).

D- Transport Layer Security (TLS).

Answer:

D

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 9

Question Type: MultipleChoice

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)?

Options:

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

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 10

Question Type: MultipleChoice

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 camer

a. 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?

Options:

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:

B

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.