DUMPSARENA

Certified Information Privacy Technologist (CIPT)

IAPP CIPT

Version Demo

Total Demo Questions: 14

Total Premium Questions: 214

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following is the least effective privacy preserving practice in the Systems Development Life Cycle (SDLC)?

A. Conducting privacy threat modeling for the use-case.

B. Following secure and privacy coding standards in the development.

C. Developing data flow modeling to identify sources and destinations of sensitive data.

D. Reviewing the code against Open Web Application Security Project (OWASP) Top 10 Security Risks.

ANSWER: C

QUESTION NO: 2

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

ANSWER: A

Explanation:

the main privacy threat posed by Radio Frequency Identification (RFID) is that it can be utilized to track people or consumer products. RFID technology allows for wireless communication between tags and readers, which can be used to track the location and movement of tagged items.

QUESTION NO: 3

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

QUESTION NO: 4

SCENARIO

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

The table below indicates some of the personal information Clean-Q requires as part of its business operations:

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

Clean-Q has an internal employee base of about 30 people. A recent privacy compliance exercise has been conducted to align employee data management and human resource functions with applicable data protection regulation. Therefore, the Clean-Q permanent employee base is not included as part of this scenario.

With an increase in construction work and housing developments, Clean-Q has had an influx of requests for cleaning services. The demand has overwhelmed Clean-Q's traditional supply and demand system that has caused some overlapping bookings.

Ina business strategy session held by senior management recently, Clear-Q invited vendors to present potential solutions to their current operational issues. These vendors included Application developers and Cloud-Q's solution providers, presenting their proposed solutions and platforms.

The Managing Director opted to initiate the process to integrate Clean-Q's operations with a cloud solution (LeadOps) that will provide the following solution one single online platform: A web interface that Clean-Q accesses for the purposes of resource and customer management. This would entail uploading resource and customer information.

 A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.

 A resource facing web interface that enables resources to apply and manage their assigned jobs.

 An online payment facility for customers to pay for services.

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

A. Nothing at this stage as the Managing Director has made a decision.

B. Determine if any Clean-Q competitors currently use LeadOps as a solution.

C. Obtain a legal opinion from an external law firm on contracts management.

D. Involve the Information Security team to understand in more detail the types of services and solutions LeadOps is proposing.

ANSWER: D

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 NO: 5

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: 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.

QUESTION NO: 6

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.

ANSWER: A

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 NO: 7

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)

ANSWER: A

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 NO: 8

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 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

ANSWER: A

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 NO: 9

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: 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 NO: 10

Machine-learning based solutions present a privacy risk because?

A. Training data used during the training phase is compromised.

B. The solution may contain inherent bias from the developers.

C. The decision-making process used by the solution is not documented.

D. Machine-learning solutions introduce more vulnerabilities than other software.

ANSWER: B

Explanation:

machine-learning based solutions present a privacy risk because they may contain inherent bias from the developers. Bias can be introduced into machine learning models through biased training data or through biased decision-making processes used by the solution.

QUESTION NO: 11

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

ANSWER: C

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 NO: 12

Which of the following statements describes an acceptable disclosure practice?

A. An organization's privacy policy discloses how data will be used among groups within the organization itself.

B. With regard to limitation of use, internal disclosure policies override contractual agreements with third parties.

C. Intermediaries processing sensitive data on behalf of an organization require stricter disclosure oversight than vendors.

D. When an organization discloses data to a vendor, the terms of the vendor' privacy notice prevail over the organization' privacy notice.

ANSWER: A

QUESTION NO: 13

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

A. The user is protected against phishing attacks.

B. The user's identity is protected from the other user.

C. The user's approximate physical location is hidden from the other user.

D. The user is assured that stronger authentication methods have been used.

ANSWER: B

QUESTION NO: 14

SCENARIO

Please use the following to answer the next question:

Chuck, a compliance auditor for a consulting firm focusing on healthcare clients, was required to travel to the client's office to perform an onsite review of the client's operations. He rented a car from Finley Motors upon arrival at the airport as so he

could commute to and from the client's office. The car rental agreement was electronically signed by Chuck and included his name, address, driver's license, make/model of the car, billing rate, and additional details describing the rental transaction. On the second night, Chuck was caught by a red light camera not stopping at an intersection on his way to dinner. Chuck returned the car back to the car rental agency at the end week without mentioning the infraction and Finley Motors emailed a copy of the final receipt to the address on file.

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

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

What is the most secure method Finley Motors should use to transmit Chuck's information to AMP Payment Resources?

A. Cloud file transfer services.

B. Certificate Authority (CA).

C. HyperText Transfer Protocol (HTTP).

D. Transport Layer Security (TLS).

ANSWER: D

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.