DUMPSQUEEN

Certified Information Privacy Technologist (CIPT)

IAPP CIPT

Version Demo

Total Demo Questions: 14

Total Premium Questions: 214

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

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: 2

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

QUESTION NO: 3

Organizations understand there are aggregation risks associated with the way the process their customer's data. They typically include the details of this aggregation risk in a privacy notice and ask that all customers acknowledge they understand these risks and consent to the processing.

What type of risk response does this notice and consent represent?

A. Risk transfer.

B. Risk mitigation.

C. Risk avoidance.

D. Risk acceptance.

ANSWER: A

QUESTION NO: 4

What element is most conducive to fostering a sound privacy by design culture in an organization?

A. Ensuring all employees acknowledge and understood the privacy policy.

B. Frequent privacy and security awareness training for employees.

C. Monthly reviews of organizational privacy principles.

D. Gaining advocacy from senior management.

ANSWER: D

Explanation:

gaining advocacy from senior management is the element most conducive to fostering a sound privacy by design culture in an organization. Senior management plays a crucial role in setting the tone and direction for privacy practices within an organization and their support is essential for establishing a strong privacy culture.

QUESTION NO: 5

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: 6

A credit card with the last few numbers visible is an example of what?

A. Masking data

B. Synthetic data

C. Sighting controls.

D. Partial encryption

ANSWER: A

Explanation:

Reference: https://money.stackexchange.com/questions/98951/credit-card-number-masking-good-practices-rules-law-regulations

QUESTION NO: 7

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.

ANSWER: B

Explanation:

the most effective and efficient way to achieve this would be to have the data encrypted at rest, and selectively decrypt it for the users who have the rights to see it.

QUESTION NO: 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."

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: C

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 NO: 9

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: 10

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: 11

SCENARIO

Please use the following to answer next question:

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

The app collects the following information:

First and last name

Date of birth (DOB)

Mailing address

Email address

Car VIN number

Car model

License plate

Insurance card number

Photo

Vehicle diagnostics

Geolocation

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

A. Peer-to-peer architecture.

B. Client-server architecture.

C. Plug-in-based architecture.

D. Service-oriented architecture.

ANSWER: D

QUESTION NO: 12

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

A. The server decrypts the PremasterSecret.

B. The web browser opens a TLS connection to the PremasterSecret.

C. The web browser encrypts the PremasterSecret with the server's public key.

D. The server and client use the same algorithm to convert the PremasterSecret into an encryption key.

ANSWER: C

Explanation:

Reference: https://books.google.com.pk/books?id=OaXise4B-p8C&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 NO: 13

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: 14

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.