



- Expert Verified, Online, **Free**.

What would be an example of an organization transferring the risks associated with a data breach?

- A. Using a third-party service to process credit card transactions.
- B. Encrypting sensitive personal data during collection and storage
- C. Purchasing insurance to cover the organization in case of a breach.
- D. Applying industry standard data handling practices to the organization' practices.

Suggested Answer: C

Reference:

<http://www.hpso.com/Documents/pdfs/newsletters/firm09-rehabv1.pdf>

Community vote distribution

C (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. Purchasing insurance to cover the organization in case of a breach.

This is an example of transferring the risks associated with a data breach. By purchasing insurance, the organization shifts some of the financial risks associated with a potential data breach to the insurance provider.

upvoted 1 times

🗳️ 👤 **valneilima** 1 year, 4 months ago

lixo mesmo

upvoted 1 times

🗳️ 👤 **ProjectBS** 1 year, 1 month ago

is this dump really no good?

upvoted 1 times

🗳️ 👤 **Erepeer** 2 years, 4 months ago

I doubt if the answers are right and the questions are outdated.

upvoted 2 times

🗳️ 👤 **837vq3** 2 years, 8 months ago

when will this dump get updated? it has the same questions since last year

upvoted 1 times

🗳️ 👤 **vicks888** 3 years, 1 month ago

how was it?

upvoted 1 times

🗳️ 👤 **837vq3** 3 years, 1 month ago

I recently took the exam and hardly got 10 questions from this dump. The dump is old and invalid.

upvoted 1 times

🗳️ 👤 **Sbowo** 3 years, 1 month ago

Yes. I already passed the exam too and got only 10-20 questions from this dump. I never believe the default answer and try to ensure it every time. This dump is good for exercising but please always question their answer.

upvoted 2 times

🗳️ 👤 **837vq3** 2 years, 8 months ago

did you find a more accurate dump from somewhere else?

upvoted 2 times

🗳️ 👤 **ProjectBS** 1 year, 1 month ago

would love to hear on accurate dump else where..

upvoted 1 times

🗳️ 👤 **ProjectBS** 10 months, 3 weeks ago

Took the exam. I think I only got 10-15 questions from this dump. Passed, nonetheless. This dump needs to be updated for sure.
upvoted 2 times

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.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. An employee stores his personal information on his company laptop.
upvoted 1 times

🗨️ 👤 **Stants** 1 year ago

The client-side IT risk among the options provided is:

C. An employee stores his personal information on his company laptop.

Client-side IT risks typically involve actions or issues related to end-users or individual devices. In this case, an employee storing personal information on a company laptop poses a potential risk to data security and confidentiality.

upvoted 2 times

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."

What type of principles would be the best guide for Jane's ideas regarding a new data management program?

- A. Collection limitation principles.
- B. Vendor management principles.
- C. Incident preparedness principles.
- D. Fair Information Practice Principles

Suggested Answer: D

Reference:

<https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/>

Community vote distribution

D (100%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Fair Information Practice Principles

upvoted 1 times

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.

Suggested Answer: A

Reference:

<https://fas.org/sgp/crs/misc/R45631.pdf>

Community vote distribution

A (50%)

C (50%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

In the context of the United States, the Federal Trade Commission (FTC) is the primary regulator overseeing consumer protection, including data privacy and security practices for businesses.

C. The Data Protection Authority would be relevant in jurisdictions where there are specific data protection authorities, such as in the European Union with GDPR. However, since Carol's shop is U.S.-based, the FTC would be the correct answer.

So, A. The Federal Trade Commission is the right choice.

upvoted 1 times

 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: C

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.

upvoted 1 times

  **JoyChada** 1 year, 6 months ago

Why not C? (I got the answer and ref from another source)

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.

upvoted 1 times

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


Suggested Answer: B

Community vote distribution

C (100%)

 **pipzz** Highly Voted 3 years, 4 months ago

C. Data minimization principles is more appropriate for this scenario. Digital rights management refers to a set of access control technologies. upvoted 6 times

 **837vq3** 3 years, 3 months ago

Minimization involves limiting the amount of personal information that needs to be processed. Ideally, this should be done at the time of collection by avoiding or preventing the collection of unnecessary information, but the concept should extend throughout the information life cycle.

upvoted 1 times

 **k4d4v4r** 3 years, 2 months ago

Anyway DRM is not for every situation in the data life cycle

upvoted 2 times

 **Ssourav** Most Recent 5 months, 3 weeks ago

Selected Answer: C


B. Digital rights management (DRM) primarily deals with the control of access to digital content and media, not the collection of personal information from customers.

In contrast, C. Data minimization principles directly relate to the collection of personal data, emphasizing the importance of collecting only what

is necessary for the intended purpose. This principle is a core aspect of privacy regulations and best practices in data management.

Therefore, C. Data minimization principles is indeed the correct answer for guiding Jane when initially collecting personal information from customers.

upvoted 1 times

  **PaigeH7** 10 months, 2 weeks ago

Selected Answer: C

When initially collecting personal information from customers, Jane should be guided by data minimization

upvoted 1 times

A key principle of an effective privacy policy is that it should be?

- A. Written in enough detail to cover the majority of likely scenarios.
- B. Made general enough to maximize flexibility in its application.
- C. Presented with external parties as the intended audience.
- D. Designed primarily by the organization's lawyers.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

The correct answer is A. Written in enough detail to cover the majority of likely scenarios.

An effective privacy policy should be detailed enough to address the most common and relevant scenarios that might arise. This helps ensure that the policy provides clear guidance on how personal data should be handled, protecting both the organization and the individuals whose data is being processed.

upvoted 2 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: A

Answer is A

upvoted 2 times

🗨️ 👤 **yaw222** 1 year, 12 months ago

Organization privacy policy is an internal documents. why this answer relate to external parties as the intended audience.

upvoted 2 times

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.

Suggested Answer: C

Community vote distribution

C (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Code of Fair Information Practice Principles (FIPPs).

The Code of Fair Information Practice Principles (FIPPs) was developed in the 1970s in the United States and is considered one of the earliest privacy frameworks. It laid the foundation for many subsequent privacy frameworks and laws around the world, including the OECD Privacy Principles and others.

upvoted 1 times

🗳️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: C

Even in the book, Introduction to Privacy for Technology, section 1.5, lists that FIPPs came out in 1977 and OECD came out in 1980

upvoted 1 times

🗳️ 👤 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: C

C. Code of Fair Information Practice Principles (FIPPs).

upvoted 1 times

🗳️ 👤 **BTAB** 2 years, 5 months ago

Selected Answer: C

Even in the book, Introduction to Privacy for Technology, section 1.5, lists that FIPPs came out in 1977 and OECD came out in 1980.

Correct answer is C.

upvoted 2 times

🗳️ 👤 **pipzz** 3 years, 4 months ago

The Fair Information Practice Principles (FIPPs) are a widely accepted framework that is at the core of the Privacy Act of 1974The FIPPs were first articulated in a comprehensive manner in the U.S. Department of Health, Education and Welfare's seminal 1973 report entitled Records, Computers and the Rights of Citizens (1973) (full-text) (hereinafter "HEW Report").In 1980, the international Organization of Economic Cooperation and Development (OECD) codified its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The original five principles set forth in the HEW Report were extended in the OECD guidelines that govern "the protection of privacy and transborder data flows of personal data" and include eight principles that have come to be understood as "minimum standards . . . for the protection of privacy and individual liberties."

https://itlaw.wikia.org/wiki/Fair_Information_Practice_Principles

upvoted 4 times

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.

Suggested Answer: D

Reference:

<https://privacyrights.org/resources/review-fair-information-principles-foundation-privacy-public-policy>

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

The OECD Privacy Principles, developed in 1980, became a foundational framework for privacy practices and principles globally. These principles have influenced many national and international privacy laws, including the EU Data Protection Directive and the General Data Protection Regulation (GDPR). They provide a comprehensive approach to privacy that has been adopted by numerous countries and organizations worldwide.

upvoted 1 times

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.

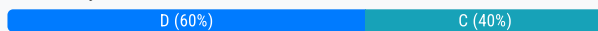
By the end of the day, Kyle was very excited about his new job and his new company. In fact, he learned about an open position for someone with strong qualifications and experience with access privileges, project standards board approval processes, and application-level obligations, and couldn't wait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

Suggested Answer: D

Community vote distribution



waterdogs 5 months, 1 week ago

Selected Answer: D

C doesnt make sense because the cyber criminals are doing authentication attacks, how would encryption of data on the network layer guard against that? chatgpt says it should be D:

"The most likely reason for Ted's implementation of a plan to encrypt data at the transportation level of the organization's wireless network would be to address the risk of data being intercepted during transmission. This suggests that the implementation is likely a response to an incident where confidential information was intercepted during communication. Therefore, the correct answer is: D. Confidential information discussed during a strategic teleconference was intercepted by the organization's top competitor."

upvoted 3 times

Ssourav 5 months, 3 weeks ago

Selected Answer: C

C. Cyber criminals accessed proprietary data by running automated authentication attacks on the organization's network is indeed a strong candidate because encryption at the transportation level (such as securing the wireless network) would be a direct response to protecting data from unauthorized access, especially within the organization's premises. This type of encryption is designed to prevent cybercriminals from intercepting or accessing data as it moves across the internal network, which aligns with the scenario described in option C.

upvoted 1 times

ChaBum 2 years, 11 months ago

Selected Answer: C

C is the only answer related to local network, and encrypting data passing through the WiFi only protect the LAN.

upvoted 3 times

ChaBum 2 years, 11 months ago

C is the only answer related to local network, and encrypting data passing through the WiFi only protect the LAN.



upvoted 1 times

  **187san** 3 years, 1 month ago

Selected Answer: D



its D , rest responses does not make sense

upvoted 3 times

  **ChaBum** 2 years, 11 months ago

teleconferences are most likely to pass through Internet because you want to interact with people outside your premises, encrypting the wireless network will only protect the data inside you premise.

upvoted 2 times

  **k4d4v4r** 3 years, 2 months ago

Why A and not D? Wireless has nothing to do with cloud

upvoted 2 times

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.

Suggested Answer: C

Community vote distribution

C (50%)

D (50%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

accidentally ticked D, answer is C
upvoted 1 times

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

The correct answer is C. Industry groups.

Industry groups are often the best source of support for initiatives related to self-regulatory privacy principles. These groups typically have established guidelines, best practices, and resources that can help organizations align with industry standards and achieve compliance. They also provide networking opportunities, which can be valuable for staying updated on the latest trends and regulatory changes.

upvoted 1 times

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

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Retention.

Barney's focus on establishing rules governing where data can be placed and minimizing the use of offline data storage suggests that he is primarily concerned with improving data retention practices. By controlling where data is stored and reducing offline storage, he is likely aiming to ensure that data is kept in secure, manageable locations and that it is retained only for as long as necessary, in compliance with the organization's data retention policies.

upvoted 1 times

🗨️ 👤 **impchoi** 1 year, 6 months ago

Chat GPT says Retention: Data retention is the practice of preserving data for a specific period of time to meet technical, business, or regulatory requirements. Any time you save data to a file, you're technically retaining it – but the term “data retention” usually refers to the deliberate, systematic ways in which you store, use, and delete data. Developing a good data retention strategy requires a solid understanding of the nature, format, sensitivity, and useful lifecycle of your data. A good place to start is to create an inventory and diagram for all your data inflows and outflows¹.

Based on this information, it seems that where data can be placed is part of retention rather than inventory.

upvoted 2 times

🗨️ 👤 **za1q2wsx** 1 year, 10 months ago

should select B

upvoted 2 times

What is the main function of a breach response center?

- A. Detecting internal security attacks.
- B. Addressing privacy incidents.
- C. Providing training to internal constituencies.
- D. Interfacing with privacy regulators and governmental bodies.

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

The correct answer is B. Addressing privacy incidents.

The main function of a breach response center is to address privacy incidents, including data breaches. This involves coordinating the response to breaches, managing communication with affected parties, and ensuring compliance with legal and regulatory requirements. While the other options are important aspects of security and privacy management, the primary focus of a breach response center is to handle incidents when they occur.

upvoted 1 times

🗨️ 👤 **Stants** 1 year ago

The main function of a breach response center is to address privacy incidents, so the answer is B. Addressing privacy incidents.

While breach response centers may have other functions, such as:

Detecting internal security attacks (to some extent, as these can lead to privacy incidents)

Providing training to internal constituencies (to help prevent future incidents)

Interfacing with privacy regulators and governmental bodies (as part of the incident response process)

Their primary focus is on handling situations where sensitive data has been compromised. This includes:

Investigating the incident to understand its scope and impact

Taking steps to contain the breach and prevent further damage

Notifying affected individuals and regulators

Implementing corrective actions to improve security

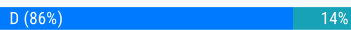
upvoted 2 times

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

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

Suggested Answer: D

Community vote distribution



pipzz Highly Voted 3 years, 4 months ago

Deletion is the main action you would take after retention periods end. The worst thing to do would be to re-tag the data.
upvoted 9 times

187san Highly Voted 3 years, 1 month ago

Selected Answer: D

D, question asked " NOT"
upvoted 6 times

Ssourav Most Recent 5 months, 3 weeks ago

Selected Answer: D

The correct answer is D. Retagging.

Retagging is not a suitable action to apply to data when the retention period ends. When data retention periods end, the data should either be deleted, de-identified, or aggregated to ensure that it no longer poses a privacy risk. Retagging would not address the need to limit access to or eliminate the data in accordance with retention policies.

upvoted 1 times

rajiabdmjd 1 year, 10 months ago

Selected Answer: D

Rettaging
upvoted 2 times

z80r 2 years ago

Selected Answer: D

I would say D
upvoted 3 times

837vq3 2 years, 4 months ago

Selected Answer: A

Aggregation
upvoted 1 times

ChaBum 2 years, 11 months ago

Selected Answer: A

Data aggregation is a process in which data is gathered and represented in a summary form, for purposes including statistical analysis. That would mean using the data after the retention period has been reached. and that does not make sense.

B. De-identification, could be a mean to keep the data under an anonymized format, and so under the condition of the collection it could make sense

C. Deletion, it the most common way to deal with data when they reach the end of their retention period.

D. Retagging, is in fact extending or resetting the retention period. For example because the PII of customers are kept for a defined retention period of 3 years EXCEPT if the customer had interaction if the Data controller during those 3 years, then the data is re-tag and kept.

upvoted 1 times

k4d4v4r 3 years, 2 months ago

C is correct. Aggregation is a common backup/retention solution. You can de-identity and you can of course retag so you can know what you can delete or what you should archive. Archive is the next step after retention.

upvoted 2 times

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.

Suggested Answer: C

Reference:

<https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties>

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. It uses distinct keys for encryption and decryption.

upvoted 1 times

What is the most important requirement to fulfill when transferring data out of an organization?

- A. Ensuring the organization sending the data controls how the data is tagged by the receiver.
- B. Ensuring the organization receiving the data performs a privacy impact assessment.
- C. Ensuring the commitments made to the data owner are followed.
- D. Extending the data retention schedule as needed.

Suggested Answer: C

Community vote distribution

C (100%)

🗉 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Ensuring the commitments made to the data owner are followed.

When transferring data out of an organization, the most important requirement is to ensure that the commitments made to the data owner (i.e., the individual whose data is being transferred) are upheld. This includes adhering to any privacy promises, data protection standards, and legal requirements that were communicated to the data owner when the data was collected. This is crucial for maintaining trust, ensuring compliance with privacy laws, and protecting the rights of the data owner.

upvoted 1 times

Which activity would best support the principle of data quality?

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

Suggested Answer: *D*

Reference:

<https://iapp.org/resources/article/fair-information-practices/>

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Ensuring that information remains accurate.

upvoted 2 times

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

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

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

The correct answer is A. Individual participation.

The Individual participation principle of the OECD privacy protection principles emphasizes the rights of individuals to have control over their personal data. This includes the ability to consent to the collection, use, and transfer of their personal information. Organizations are encouraged to obtain consent from individuals before transferring their personal information, in alignment with this principle.

upvoted 2 times

🗨️ 👤 **ofirga** 11 months, 3 weeks ago

The right answer is C. You can see evidence here: https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

upvoted 2 times

🗨️ 👤 **PTDT** 1 year, 4 months ago

Selected Answer: A

It is A.

upvoted 2 times

🗨️ 👤 **Stants** 1 year ago

A. Individual participation.

The Organization for Economic Co-operation and Development (OECD) privacy protection principle that encourages an organization to obtain an individual's consent before transferring personal information is "Individual participation." This principle emphasizes the importance of allowing individuals to have a say in the use and disclosure of their personal data, including providing consent for the transfer of their information to third parties.

upvoted 1 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

Why isn't it A?

upvoted 2 times

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

Suggested Answer: D

Reference:

<https://www.ncbi.nlm.nih.gov/books/NBK236546/>

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

The correct answer is D. Individual participation.

Individual participation refers to the rights of data subjects to have a say in how their personal data is handled. This includes the right to access, correct, amend, or delete their data. Granting these rights ensures that individuals have control over their personal information, which is a key aspect of the individual participation principle in data protection frameworks.

upvoted 2 times

🗨️ 👤 **Stants** 1 year ago

D. Individual participation.

Granting data subjects the right to have data corrected, amended, or deleted aligns with the principle of "Individual participation." This principle emphasizes the importance of individuals having control over their own personal data, including the ability to request corrections or deletions when necessary. It is a key aspect of privacy and data protection frameworks that prioritize giving individuals a say in how their information is managed.

upvoted 1 times


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

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

Suggested Answer: D

Community vote distribution

D (100%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

The correct answer is D. Failing to get explicit consent from a user on the use of cookies.

One common mistake organizations make when establishing privacy settings during the development of applications is failing to obtain explicit consent from users regarding the use of cookies. Explicit consent is a key requirement under many privacy regulations, such as the GDPR, which mandates that users must be informed and give clear consent before cookies or similar technologies are used to track their activities.

upvoted 1 times

 **steven2xx** 1 year, 8 months ago

if the application doesn't use cookie at all, why they should get the consent?

upvoted 2 times



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.

Suggested Answer: *D*

Community vote distribution

D (100%)

  **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

The correct answer is D. After reading the privacy notice, a data subject confidently infers how her information will be used.

This option suggests the greatest degree of transparency because it indicates that the privacy notice is clear and specific enough that the data subject fully understands how their information will be used. Transparency is achieved when individuals can easily comprehend what will happen to their data without ambiguity or confusion.

upvoted 2 times

Which is NOT a suitable method for assuring the quality of data collected by a third-party company?

- A. Verifying the accuracy of the data by contacting users.
- B. Validating the company's data collection procedures.
- C. Introducing erroneous data to see if its detected.
- D. Tracking changes to data through auditing.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Introducing erroneous data to see if it's detected.

This method is not suitable for assuring the quality of data collected by a third-party company because it involves intentionally introducing false data, which could create confusion, legal issues, or harm the integrity of the data set. The other methods—verifying accuracy, validating procedures, and tracking changes through auditing—are all legitimate ways to ensure data quality.

upvoted 1 times

🗨️ **ofirga** 11 months, 3 weeks ago

The answer is C.

The method that is NOT suitable for assuring the quality of data collected by a third-party company is C. Introducing erroneous data to see if it's detected. While it might seem like a way to test the system, intentionally introducing incorrect data can lead to unintended consequences and potentially harm the accuracy and reliability of the collected information. Instead, focus on other methods like verifying accuracy, validating procedures, and tracking changes through auditing to ensure data quality.

upvoted 1 times

🗨️ **rajiabdmjd** 1 year, 10 months ago

Selected Answer: C

C. Introducing erroneous data to see if it's detected.

Introducing erroneous data to see if it's detected is not a suitable method for assuring the quality of data collected by a third-party company. This approach is likely to introduce additional errors into the data and may not provide a reliable measure of the quality of the data. Suitable methods for assuring the quality of data collected by a third-party company include verifying the accuracy of the data by contacting users, validating the company's data collection procedures, and tracking changes to data through auditing. These methods can help to ensure that the data collected is accurate, complete, and reliable, which is important for making informed decisions based on that data.

upvoted 2 times

🗨️ **z80r** 2 years ago

Selected Answer: C

C guys

upvoted 2 times

🗨️ **Sara_sw** 2 years, 2 months ago

Selected Answer: C

The question asks which is NOT the correct approach.

A is correct, C is NOT correct so the answer is C

upvoted 3 times

🗨️ **Sbowo** 3 years, 1 month ago



C is NOT correct, see page 63 book Privacy in Technology by Cannon

upvoted 2 times

🗨️ **k4d4v4r** 3 years, 2 months ago



A is correct then

upvoted 2 times

  **k4d4v4r** 3 years, 2 months ago

A is absurd and would be a privacy violation

upvoted 1 times

  **837vq3** 3 years, 3 months ago

Why not "B" "Introducing erroneous data to see if its detected."?

upvoted 2 times

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.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

The correct answer is A. Can limit business opportunities.

Data minimization involves collecting and retaining only the data that is strictly necessary for a specific purpose. While this is beneficial from a privacy and security standpoint, a valid argument against it is that it can limit business opportunities. By restricting the amount of data collected, organizations might miss out on potential insights or opportunities that could arise from having a broader data set.

upvoted 2 times

What is the main reason a company relies on implied consent instead of explicit consent from a user to process her data?

- A. The implied consent model provides the user with more detailed data collection information.
- B. To secure explicit consent, a user's website browsing would be significantly disrupted.
- C. An explicit consent model is more expensive to implement.
- D. Regulators prefer the implied consent model.

Suggested Answer: B

Community vote distribution

B (100%)

 **Sbowo** Highly Voted 3 years, 1 month ago

B is the answer based on the book
upvoted 6 times


 **Ssourav** Most Recent 5 months, 3 weeks ago

Selected Answer: B

The correct answer is B. To secure explicit consent, a user's website browsing would be significantly disrupted.

One of the main reasons companies rely on implied consent rather than explicit consent is to minimize disruption to the user's experience. Securing explicit consent often requires interrupting the user's activity with consent requests, pop-ups, or other forms of interaction, which can negatively impact the browsing experience. Implied consent allows the company to process data in a way that is less intrusive, although it is important to ensure that this approach complies with applicable legal requirements.

upvoted 2 times

 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: B

Explicit consent typically involves more active steps, such as clicking checkboxes or providing specific permissions, which can interrupt the user experience.

upvoted 1 times

 **ofirga** 11 months, 3 weeks ago

The answer is B

The main reason a company relies on implied consent instead of explicit consent from a user to process their data is typically due to the concern that securing explicit consent might significantly disrupt the user's website browsing experience. Implied consent assumes that users agree to certain data processing practices by continuing to use a website or service, without requiring them to actively provide explicit consent for each specific action. While explicit consent provides more transparency and control to users, it can indeed be more cumbersome to implement and may lead to interruptions in the user experience. However, companies must strike a balance between user privacy and operational efficiency while adhering to relevant regulations. □

upvoted 1 times

 **Stants** 1 year ago

B. Disruption: Explicit consent typically requires users to actively opt-in or out through prompts or checkboxes, which can interrupt their browsing experience and reduce engagement. Implied consent allows for smoother user flow on websites and applications.

upvoted 1 times

 **steven2xx** 1 year, 8 months ago

why is C?

upvoted 1 times

 **rajiabdmjd** 1 year, 10 months ago

B should be the correct answer

upvoted 1 times

 **steven222223** 1 year, 10 months ago

which part?

upvoted 2 times

What is the main benefit of using dummy data during software testing?

- A. The data comes in a format convenient for testing.
- B. Statistical disclosure controls are applied to the data.
- C. The data enables the suppression of particular values in a set.
- D. Developers do not need special privacy training to test the software.

Suggested Answer: D

Community vote distribution

D (67%)

C (33%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

Dummy data is typically fabricated or non-sensitive data used to simulate real data in a testing environment. The main purpose of using dummy data is to allow developers to test the functionality of software without risking exposure to sensitive or personally identifiable information (PII).

B and C involve protecting or managing real data, which is not the point of dummy data. These techniques are used when real data is being anonymized or when privacy controls are being applied to actual datasets.

D correctly identifies that with dummy data, developers do not need to handle real personal data, which reduces the need for specialized privacy training related to data protection laws and regulations.

upvoted 2 times

🗨️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: C

Dummy data allows testers to create controlled scenarios by intentionally including or excluding specific values, ensuring comprehensive test coverage without compromising sensitive information. It helps protect privacy and maintain data security during testing.

upvoted 1 times

🗨️ 👤 **ofirga** 11 months, 3 weeks ago

The answer is A.

The main benefit of using dummy data during software testing is that it allows developers to create realistic scenarios without exposing real user information. Let's break down the options:

A. The data comes in a format convenient for testing.

This is true. Dummy data can be customized to simulate various scenarios, making it convenient for testing different functionalities.

upvoted 1 times

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."

Suggested Answer: A

Reference:

https://www.researchgate.net/publication/284332229_k-Anonymity_A_Model_for_Protecting_Privacy

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

The correct answer is A. By ensuring that every record in a set is part of a group of "k" records having similar identifying information.

K-anonymity is a method used to protect privacy in microdata sets by ensuring that each record is indistinguishable from at least

k

-

1

k-1 other records with respect to certain identifying attributes. This means that any single record cannot be uniquely identified within the dataset, as it shares the same values for key identifying fields with at least

k

k other records. This reduces the risk of re-identification of individuals within the dataset.

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 3 months ago

k-anonymity relies on the creation of generalized, truncated, or redacted quasi-identifiers as replacements for direct identifiers such that a given minimum number ("k") of individuals in a data set have the same identifier

upvoted 1 times

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.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

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

This statement describes an acceptable disclosure practice because it aligns with the principle of transparency in data handling within an organization. It is important for organizations to clearly communicate how data will be used, including how it is shared internally among different groups or departments, to ensure that data subjects are aware of how their information is being handled.

The other options either contradict best practices (like overriding contractual agreements or giving precedence to a vendor's privacy notice over the organization's) or are less relevant to standard disclosure practices.

upvoted 1 times

🗨️ 👤 **4n0nym3** 9 months, 2 weeks ago

Why not D? Isn't A a bit too detailed for the data subjects?

upvoted 2 times

How should the sharing of information within an organization be documented?


- A. With a binding contract.
- B. With a data flow diagram.
- C. With a disclosure statement.
- D. With a memorandum of agreement.

Suggested Answer: B

Community vote distribution

B (80%)

D (20%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

The correct answer is B. With a data flow diagram.

A data flow diagram is a visual representation that shows how data moves within an organization, including how information is shared between different departments or systems. It is an effective way to document the sharing of information within an organization, as it provides a clear and understandable overview of data processes, helping to ensure transparency and compliance with data protection practices.

upvoted 1 times

 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: D

The sharing of information within an organization is typically documented with a memorandum of agreement (MOA). An MOA outlines the terms, responsibilities, and expectations related to information sharing between parties. It serves as a formal record of the agreement and helps ensure clarity and accountability.

upvoted 1 times

 **ofirga** 11 months, 3 weeks ago

The answer is D.

The sharing of information within an organization should be documented with a memorandum of agreement (MOA). An MOA outlines the terms, responsibilities, and expectations related to information sharing between parties. It serves as a formal record of the agreement and helps ensure clarity and accountability. While other options (such as binding contracts, data flow diagrams, and disclosure statements) may play roles in specific contexts, an MOA specifically addresses the sharing of information.

upvoted 2 times

 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: B

A data flow diagram is a graphical representation of the flow of data within a system or organization. While it can be used to document the flow of information within an organization, it may not be the most suitable or comprehensive method for documenting the sharing of information.

A data flow diagram can be useful in illustrating how information moves through a system or process, but it may not capture all the necessary details related to data sharing, such as the types of data being shared, the purpose of sharing, and the security measures in place to protect the data.

Therefore, while a data flow diagram may be part of the documentation for sharing information within an organization, it is not typically the sole or primary method used for documenting data sharing.

upvoted 3 times

 **rajiabdmjd** 1 year, 10 months ago

Why not B ?

upvoted 2 times

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

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

Suggested Answer: *D*

Reference:

<https://cloud.google.com/storage/docs/gsutil/addlhelp/WorkingWithObjectMetadata>

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Metadata.

upvoted 1 times

What must be done to destroy data stored on "write once read many" (WORM) media?


- A. The data must be made inaccessible by encryption.
- B. The erase function must be used to remove all data.
- C. The media must be physically destroyed.
- D. The media must be reformatted.

Suggested Answer: C

Community vote distribution

C (100%)



 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. The media must be physically destroyed.

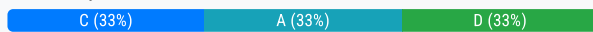
upvoted 1 times

Which of the following would best improve an organization's system of limiting data use?

- A. Implementing digital rights management technology.
- B. Confirming implied consent for any secondary use of data.
- C. Applying audit trails to resources to monitor company personnel.
- D. Instituting a system of user authentication for company personnel.

Suggested Answer: C

Community vote distribution



🗨️ **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. Applying audit trails to resources to monitor company personnel goes beyond just controlling access—it actively monitors and records how data is used after access is granted. This is crucial for limiting data use because it provides a mechanism to detect and respond to any misuse or unauthorized use of data within the organization.

In summary:

A and D are about controlling access and rights, but C specifically focuses on limiting data use by providing continuous oversight through monitoring and auditing, making it the best option for improving the system of limiting data use.

upvoted 1 times

🗨️ **PaigeH7** 10 months, 2 weeks ago

Selected Answer: A

DRM helps control access to digital content and restricts how data is used, ensuring that only authorized individuals can access and manipulate it.

upvoted 1 times

🗨️ **rajiabdmjd** 1 year, 10 months ago

Selected Answer: D

Instituting a system of user authentication for company personnel.

upvoted 1 times

🗨️ **rajiabdmjd** 1 year, 10 months ago

I think D

upvoted 1 times

🗨️ **Sbowo** 3 years, 1 month ago

Answer is D, based on Privacy in Technology book. All answer is correct, but base on priority, first one is explicit consent on secondary use, second is user authentication

upvoted 3 times

🗨️ **k4d4v4r** 3 years, 2 months ago

C is correct. DRM is more related to end users. For systems you should rely on audit logs to monitor usage of data.

upvoted 2 times

🗨️ **837vq3** 3 years, 3 months ago

Digital Rights Management: This is used to ensure that digital content is only delivered to those who are authorized to receive it. It can also limit what assigned

users can do with the content. For example, a person may be permitted to read a

© International Association of Privacy Professionals 10

the document, but not allowed to print it, email it to others, copy content from it or modify it.

upvoted 1 times

Which of the following is considered a records management best practice?

- A. Archiving expired data records and files.
- B. Storing decryption keys with their associated backup systems.
- C. Implementing consistent handling practices across all record types.
- D. Using classification to determine access rules and retention policy.

Suggested Answer: D

Reference:

<https://www.archive-vault.co.uk/best-practice-for-records-management>

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Using classification to determine access rules and retention policy.

upvoted 1 times

Which of the following provides a mechanism that allows an end-user to use a single sign-on (SSO) for multiple services?


- A. The Open ID Federation.
- B. PCI Data Security Standards Council
- C. International Organization for Standardization.
- D. Personal Information Protection and Electronic Documents Act.

Suggested Answer: A

Community vote distribution

A (100%)



 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. The Open ID Federation.

upvoted 1 times

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.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Discretionary access control.

Discretionary access control (DAC) is a type of access control where the owner of a resource (e.g., a file or database) has the discretion to decide who can access that resource and what kind of access they can have. The owner can grant or revoke permissions to other users based on their own criteria.

upvoted 1 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

Correct answer is C

upvoted 1 times

🗨️ 👤 **837vq3** 2 years, 4 months ago

Selected Answer: C

C is the answer

upvoted 2 times

🗨️ 👤 **ChaBum** 2 years, 11 months ago

Selected Answer: C

Here is the definition of DAC from iapp: A type of access control that allows an owner of an object, within a given computer-based information system, to grant or deny access.

upvoted 3 times

🗨️ 👤 **Sbowo** 3 years, 1 month ago

C is the answer

upvoted 4 times

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.

Suggested Answer: A

Community vote distribution

A (78%)

C (22%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

The correct answer is A. Encrypted information can be analyzed without decrypting it first.

Homomorphic encryption allows computations to be performed on encrypted data without needing to decrypt it first. The results of these computations, when decrypted, match the results as if they had been performed on the unencrypted data. This feature enables secure data analysis and processing while maintaining privacy, making it a highly valuable technique in scenarios where sensitive data needs to be processed or analyzed without exposing it to potential threats.

upvoted 1 times

🗨️ 👤 **4n0nym3** 9 months, 2 weeks ago

Definitely A.

C doesn't make sense performance wise, it'll just add computation overhead

upvoted 1 times

🗨️ 👤 **z80r** 2 years ago

Selected Answer: A

it's A for sure

upvoted 2 times

🗨️ 👤 **z80r** 2 years ago

Selected Answer: C

it's C

upvoted 2 times

🗨️ 👤 **ChaBum** 2 years, 11 months ago

Selected Answer: A

Definition of Homomorphic from iapp: Allows encrypted information to be manipulated without first being decrypted.

upvoted 2 times

🗨️ 👤 **Sbowo** 3 years, 1 month ago

A is the answer

upvoted 2 times

🗨️ 👤 **187san** 3 years, 1 month ago

Selected Answer: A

Homomorphic encryption is a form of encryption that permits users to perform computations on its encrypted data without first decrypting it. ... This allo while encrypted.

[https://en.wikipedia.org/wiki/Homomorphic_encryption#:~:text=Homomorphic%20encryption%20is%20a%20form,data%20without%20first%20decrypting%](https://en.wikipedia.org/wiki/Homomorphic_encryption#:~:text=Homomorphic%20encryption%20is%20a%20form,data%20without%20first%20decrypting%20)

upvoted 2 times

🗨️ 👤 **k4d4v4r** 3 years, 2 months ago

A should be correct. "Faster processing times" is tremendously erroneous for homomorphic encryption

upvoted 2 times

🗨️ 👤 **837vq3** 3 years, 2 months ago

Homomorphic encryption allows encrypted information to be manipulated without first being decrypted. Early homomorphic encryption was too slow to be of practical use but is now fast enough to use with some applications that require high degrees of privacy and security.

upvoted 2 times

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.

Suggested Answer: C

Community vote distribution

C (100%)

 **Sbowo** Highly Voted 3 years, 1 month ago

I think C is the answer because disreputable CA will make their certificate questionable
upvoted 6 times

 **Ssourav** Most Recent 5 months, 3 weeks ago

Selected Answer: C

The correct answer is C. Disreputable certificate authorities.

Disreputable certificate authorities (CAs) can undermine the public key infrastructure (PKI) system. PKI relies on trusted certificate authorities to issue and manage digital certificates that verify the identity of entities (such as websites). If a CA is compromised or behaves unethically, it can issue fraudulent certificates, leading to a breakdown in trust within the PKI system. This can result in security breaches, such as man-in-the-middle attacks, where attackers can impersonate legitimate entities.

While the other options describe potential security issues, the integrity and trustworthiness of certificate authorities are fundamental to the overall security of PKI.

upvoted 2 times

 **FayBab1** 1 year, 2 months ago

Agree about C ... D is a local impact

upvoted 2 times

 **pipzz** 2 years, 6 months ago

Selected Answer: C

Privacy for Technology book also mentions when DigiNotar, a Dutch CA owned by VASCO Data Security International, apparently issued a certificate for the domain name *.google.com. The problem is that DigiNotar didn't issue the certificate to Google—it appears that it was issued by the government of Iran, which allegedly used the certificate to spy on Iranian citizens accessing Gmail and Google docs.

upvoted 3 times

SCENARIO -

Wesley Energy has finally made its move, acquiring the venerable oil and gas exploration firm Lancelot from its long-time owner David Wilson. As a member of the transition team, you have come to realize that Wilson's quirky nature affected even Lancelot's data practices, which are maddeningly inconsistent. 'The old man hired and fired IT people like he was changing his necktie,' one of Wilson's seasoned lieutenants tells you, as you identify the traces of initiatives left half complete.

For instance, while some proprietary data and personal information on clients and employees is encrypted, other sensitive information, including health information from surveillance testing of employees for toxic exposures, remains unencrypted, particularly when included within longer records with less-sensitive data. You also find that data is scattered across applications, servers and facilities in a manner that at first glance seems almost random.

Among your preliminary findings of the condition of data at Lancelot are the following:

- ⇒ Cloud technology is supplied by vendors around the world, including firms that you have not heard of. You are told by a former Lancelot employee that these vendors operate with divergent security requirements and protocols.
- ⇒ The company's proprietary recovery process for shale oil is stored on servers among a variety of less-sensitive information that can be accessed not only by scientists, but by personnel of all types at most company locations.
- ⇒ DES is the strongest encryption algorithm currently used for any file.
- ⇒ Several company facilities lack physical security controls, beyond visitor check-in, which familiar vendors often bypass.
- ⇒ Fixing all of this will take work, but first you need to grasp the scope of the mess and formulate a plan of action to address it.

Which is true regarding the type of encryption Lancelot uses?

- A. It employs the data scrambling technique known as obfuscation.
- B. Its decryption key is derived from its encryption key.
- C. It uses a single key for encryption and decryption.
- D. It is a data masking methodology.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. It uses a single key for encryption and decryption.

This is because DES (Data Encryption Standard), which is mentioned in the scenario, is a symmetric encryption algorithm. Symmetric encryption uses the same key for both encryption and decryption.

upvoted 1 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

Correct

upvoted 1 times

SCENARIO -

Wesley Energy has finally made its move, acquiring the venerable oil and gas exploration firm Lancelot from its long-time owner David Wilson. As a member of the transition team, you have come to realize that Wilson's quirky nature affected even Lancelot's data practices, which are maddeningly inconsistent. `The old man hired and fired IT people like he was changing his necktie,` one of Wilson's seasoned lieutenants tells you, as you identify the traces of initiatives left half complete.

For instance, while some proprietary data and personal information on clients and employees is encrypted, other sensitive information, including health information from surveillance testing of employees for toxic exposures, remains unencrypted, particularly when included within longer records with less-sensitive data. You also find that data is scattered across applications, servers and facilities in a manner that at first glance seems almost random.

Among your preliminary findings of the condition of data at Lancelot are the following:

- ⇒ Cloud technology is supplied by vendors around the world, including firms that you have not heard of. You are told by a former Lancelot employee that these vendors operate with divergent security requirements and protocols.
- ⇒ The company's proprietary recovery process for shale oil is stored on servers among a variety of less-sensitive information that can be accessed not only by scientists, but by personnel of all types at most company locations.
- ⇒ DES is the strongest encryption algorithm currently used for any file.
- ⇒ Several company facilities lack physical security controls, beyond visitor check-in, which familiar vendors often bypass.
- ⇒ Fixing all of this will take work, but first you need to grasp the scope of the mess and formulate a plan of action to address it.

Which procedure should be employed to identify the types and locations of data held by Wesley Energy?

- A. Privacy audit.
- B. Log collection
- C. Data inventory.
- D. Data classification.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. Data inventory.

upvoted 1 times

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

Suggested Answer: A

Reference:

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

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Masking data
upvoted 1 times

What is an example of a just-in-time notice?

- A. A warning that a website may be unsafe.
- B. A full organizational privacy notice publicly available on a website
- C. A credit card company calling a user to verify a purchase before it is authorized
- D. Privacy information given to a user when he attempts to comment on an online article.

Suggested Answer: D

Reference:

<https://www.clarip.com/data-privacy/just-time-notice/>

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Privacy information given to a user when he attempts to comment on an online article.

upvoted 2 times

🗨️ 👤 **steven2xx** 1 year, 8 months ago

why A is wrong?

upvoted 1 times

🗨️ 👤 **waterdogs** 5 months, 1 week ago

'just in time' notice is sepcifically describing privacy notices given to people, A is about general warnings about website safety

upvoted 2 times

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.

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Update the contract to bring the vendor into alignment.
upvoted 1 times

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.

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Record encryption is granular, limiting the damage of potential breaches.

Record encryption offers a more granular approach to data security, meaning that if a breach occurs, only the specific records that were compromised are affected, rather than larger chunks of data that might be encrypted at the disk, file, or table level. This approach minimizes the impact of a potential breach.

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 3 months ago

In record encryption, records are encrypted one record at a time.

This provides enhanced protection because the protection is more granular; however, record encryption may cause performance issues because encrypting and decrypting data can be time-consuming.

upvoted 2 times

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.

What measures can protect client information stored at GFDC?

- A. De-linking of data into client-specific packets.
- B. Cloud-based applications.
- C. Server-side controls.
- D. Data pruning

Suggested Answer: A

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. Server-side controls.

Server-side controls are essential for protecting client information stored at GFDC. These controls include measures like strong authentication, encryption, access controls, and monitoring, which are critical for ensuring the security and integrity of the data stored on the servers.

A. De-linking of data into client-specific packets and D. Data pruning could also be helpful, but they are more specific techniques and not as broad or fundamental as server-side controls. B. Cloud-based applications may offer certain security features, but they are not inherently a security measure without proper implementation and controls.

upvoted 1 times

🗨️ 👤 **steven2xx** 1 year, 8 months ago

why not C?

upvoted 1 times

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.

What type of wireless network does GFDC seem to employ?

- A. A hidden network.
- B. A reluctant network.
- C. A user verified network.
- D. A wireless mesh network.

Suggested Answer: A

Reference:

<https://help.gnome.org/users/gnome-help/stable/net-wireless-hidden.html.en>*Community vote distribution*A (100%)

🗉 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

The correct answer is:

A. A hidden network.

The scenario describes a situation where the wireless network does not appear in the list of available networks but can be found when searched by name. This indicates that GFDC is using a hidden network, which is not broadcasted openly to avoid detection.

upvoted 1 times

What must be used in conjunction with disk encryption?

- A. Increased CPU speed.
- B. A strong password.
- C. A digital signature.
- D. Export controls.

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. A strong password.

Disk encryption protects data at rest by encrypting the entire disk or volume. However, encryption alone is not sufficient; a strong password (or passphrase) is necessary to protect the encryption key and ensure that only authorized users can access the encrypted data. This combination enhances security by preventing unauthorized access to the encrypted data.

upvoted 1 times

🗳️ 👤 **SMHcalicut** 1 year, 5 months ago

You can use digital signatures to authenticate data stored on an encrypted disk. For example, you could digitally sign important files or system configurations stored on an encrypted disk. This helps ensure that even if an attacker gains access to the encrypted data, they cannot modify the data without detection.

upvoted 1 times

🗳️ 👤 **rajiabdmjd** 1 year, 10 months ago

Strong password

upvoted 1 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: B

I confirm, B is the answer

upvoted 3 times

🗳️ 👤 **837vq3** 2 years, 4 months ago

Selected Answer: B

disk encryption would need password

upvoted 3 times

🗳️ 👤 **Sbowo** 3 years, 1 month ago

B is the answer because disc encryption is useless without strong password

upvoted 2 times

🗳️ 👤 **ChaBum** 2 years, 11 months ago

(full) disk encryption is based on digital certificate and not password

upvoted 1 times

🗳️ 👤 **SamPhil** 2 years, 5 months ago

That is incorrect, disk encryption is based on symmetric encryption and not public key cryptography. Digital certificate is a technology that uses public key cryptography.

upvoted 3 times

Which is NOT a way to validate a person's identity?

- A. Swiping a smartcard into an electronic reader.
- B. Using a program that creates random passwords.
- C. Answering a question about "something you know".
- D. Selecting a picture and tracing a unique pattern on it

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Using a program that creates random passwords.

Creating random passwords is a method for generating strong credentials but does not directly validate a person's identity. The other options—swiping a smartcard, answering a security question, and tracing a unique pattern—are methods used to verify or authenticate a person's identity.

upvoted 1 times

🗨️ 👤 **Ame123456789** 1 year, 10 months ago

I dont really understand D. How can you identify a person by getting him to select a person and do tracing?

upvoted 1 times

🗨️ 👤 **jrhd84** 9 months, 3 weeks ago

Because the pattern is created by the user. This was the security used on most android smart phones not too long ago.

upvoted 1 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

This is used by Microsoft on Windows device to verify users.

upvoted 1 times

Revocation and reissuing of compromised credentials is impossible for which of the following authentication techniques?

- A. Biometric data.
- B. Picture passwords.
- C. Personal identification number.
- D. Radio frequency identification.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Biometric data.

Biometric data, such as fingerprints or iris scans, cannot be easily revoked and reissued. Unlike passwords or smartcards, biometric characteristics are unique to an individual and cannot be changed if compromised. If biometric data is compromised, it would require significant changes in how identity verification is handled or new biometric data altogether, which is not practically feasible.

upvoted 1 times

🗨️ 👤 **MutantHeadcase** 1 year, 7 months ago

Selected Answer: A

Some of the answers on this site are very odd, including this one. Biometric data can be but not radio frequency????

upvoted 1 times

🗨️ 👤 **ChaBum** 2 years, 11 months ago

Selected Answer: A

Except Biometric data which are part of an individual, it's fully possible to discard and re-issue Picture passwords, PIN or RFID badge

upvoted 4 times

🗨️ 👤 **187san** 3 years, 1 month ago

A its A

upvoted 4 times

🗨️ 👤 **837vq3** 3 years, 2 months ago

Selected Answer: A

It is "A". You can't revoke biometric data.

<https://www.ciodive.com/news/you-cant-revoke-your-fingerprint/449088/>

<https://www.pentestpartners.com/security-blog/biometric-revocation-not-an-option/>

upvoted 4 times

🗨️ 👤 **837vq3** 3 years, 2 months ago

why not "A"?

upvoted 2 times

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.

Suggested Answer: A

Reference:

<https://www.wired.co.uk/article/tails-operating-software>

Community vote distribution

A (67%)

B (33%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. It allows the user to run a self-contained computer from a USB device.

The Amnesic Incognito Live System (TAILS) is a live operating system that you can run from a USB stick or DVD. It is designed to preserve privacy and anonymity by not leaving traces on the computer you're using. It does not save any data to the hard drive and is self-contained, which aligns with option A.

upvoted 2 times

🗨️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: B

The correct answer is B. It accesses systems with a credential that leaves no discernable tracks. TAILS is designed to provide anonymous and private internet usage by running from a USB device without leaving traces on the host system. It routes internet traffic through the Tor network, ensuring privacy and security for users who need to browse or communicate without revealing their identity or leaving digital footprints. TAILS does not suspend security protocols; instead, it enhances security by minimizing exposure and maintaining anonymity.

upvoted 1 times

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.

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. It is difficult for people to use.

Biometric recognition systems are generally designed to be user-friendly and intuitive, making them relatively easy for most people to use. In contrast, drawbacks of biometric systems often include higher maintenance and support needs, higher costs, and limited compatibility across different systems.

upvoted 1 times

🗳️ 👤 **Ame123456789** 1 year, 10 months ago

Should be D. "not a drawback" = not a difficult task, imo.

upvoted 1 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: D

D it's the right one imho

upvoted 1 times

🗳️ 👤 **Sbowo** 3 years, 1 month ago

D it is easy to use

upvoted 2 times

🗳️ 👤 **187san** 3 years, 1 month ago

C

Its not difficult to use

upvoted 2 times

🗳️ 👤 **k4d4v4r** 3 years, 1 month ago

Selected Answer: D

D is better

upvoted 3 times

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.

Suggested Answer: D

Community vote distribution

D (86%)

14%

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. It is a good way to achieve de-identification and unlinkability.

Data aggregation involves combining data from multiple sources to produce summary information or patterns. A main benefit of this process is that it can help achieve de-identification by removing or generalizing specific details, thereby reducing the risk of identifying individual data subjects and enhancing unlinkability. This is particularly valuable for protecting privacy while still allowing for useful analysis.

Data aggregation typically combines large datasets to provide a broader perspective or summary insights. It helps in drawing conclusions from comprehensive data rather than small samples so answer C is not accurate,
upvoted 2 times

🗳️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: C

he correct answer is C. It allows one to draw valid conclusions from small data samples. Data aggregation simplifies the complexity of large datasets, making it easier to analyze and interpret. By summarizing data, organizations can identify trends and patterns, leading to informed decision-making. While it doesn't directly eliminate the need for statisticians, it enhances efficiency and provides meaningful insights from aggregated data
upvoted 1 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: D

I think D is the correct answer
upvoted 2 times

🗳️ 👤 **837vq3** 2 years, 4 months ago

When data is aggregated, information is expressed in a summary form that reduces the value and quality of the data as well as the connection between the data and the individual it belongs to.
While using aggregation may reduce privacy concerns, it is often still possible to determine individual values from aggregated statistics.
upvoted 1 times

🗳️ 👤 **Magim1920** 2 years, 7 months ago

Selected Answer: D

Aggregation is applied to make data less identifiable
upvoted 1 times

🗳️ 👤 **187san** 3 years, 1 month ago

Selected Answer: D

D is the answer
upvoted 1 times

🗳️ 👤 **ChaBum** 2 years, 11 months ago

Data aggregation is a process in which data is gathered and represented in a summary form, for purposes including statistical analysis.
upvoted 1 times

Under the Family Educational Rights and Privacy Act (FERPA), releasing personally identifiable information from a student's educational record requires written permission from the parent or eligible student in order for information to be?

- A. Released to a prospective employer.
- B. Released to schools to which a student is transferring.
- C. Released to specific individuals for audit or evaluation purposes.
- D. Released in response to a judicial order or lawfully ordered subpoena.

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

- A. Released to a prospective employer. - Requires written permission.
- B. Released to schools to which a student is transferring. - Does not require written permission as this is an exception under FERPA.
- C. Released to specific individuals for audit or evaluation purposes. - Does not require written permission under FERPA, as long as it is for specific purposes related to audit or evaluation.
- D. Released in response to a judicial order or lawfully ordered subpoena. - Does not require written permission but does require that the institution make a reasonable effort to notify the student or parent before complying.

upvoted 1 times

🗳️ 👤 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: A

- A. Released to a prospective employer.

upvoted 1 times

🗳️ 👤 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: A

The answer is A

upvoted 1 times

🗳️ 👤 **rajiabdmjd** 1 year, 10 months ago

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

upvoted 1 times

🗳️ 👤 **Sara_sw** 2 years, 2 months ago

Selected Answer: A

A is correct since all other options are listed in the reference as NOT requiring consent

upvoted 1 times

🗳️ 👤 **187san** 3 years, 1 month ago

A is the answer

upvoted 2 times

🗨️ 👤 **187san** 3 years, 1 month ago

D , To comply with a judicial order or lawfully issued subpoena;

Check reference llink

upvoted 1 times

🗨️ 👤 **k4d4v4r** 3 years, 2 months ago

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

School officials with legitimate educational interest;

Other schools to which a student is transferring;

Specified officials for audit or evaluation purposes;

Appropriate parties in connection with financial aid to a student;

Organizations conducting certain studies for or on behalf of the school;

Accrediting organizations;

To comply with a judicial order or lawfully issued subpoena;

Appropriate officials in cases of health and safety emergencies; and

State and local authorities, within a juvenile justice system, pursuant to specific State law.

upvoted 1 times

After committing to a Privacy by Design program, which activity should take place first?

- A. Create a privacy standard that applies to all projects and services.
- B. Establish a retention policy for all data being collected.
- C. Implement easy to use privacy settings for users.
- D. Perform privacy reviews on new projects.

Suggested Answer: A

Community vote distribution

A (88%) 13%

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Create a privacy standard that applies to all projects and services.

Before implementing specific privacy measures or conducting reviews, it's essential to establish a comprehensive privacy standard that provides a framework for how privacy will be managed across all projects and services. This standard ensures consistency and alignment with privacy principles throughout the organization. Once the standard is in place, you can then move on to setting retention policies, implementing privacy settings, and performing privacy reviews.

upvoted 2 times

🗳️ 👤 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: A

A is correct

upvoted 1 times

🗳️ 👤 **rajiabdmjd** 1 year, 10 months ago

A is correct

upvoted 1 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: A

I think A

upvoted 1 times

🗳️ 👤 **Magim1920** 2 years, 7 months ago

Selected Answer: D

Performing privacy reviews on new projects constitutes performing DPIAs on new projects, which is a critical element of privacy by design - identifying privacy risks and their impact is the only way to implement safeguards in an early stadium.

upvoted 1 times

🗳️ 👤 **Sbowo** 3 years, 1 month ago

Create a privacy standard, page 130 book Privacy in Technology

upvoted 2 times

🗳️ 👤 **187san** 3 years, 1 month ago

A

is the answer

upvoted 1 times

🗳️ 👤 **k4d4v4r** 3 years, 1 month ago

The problem with A is the word "standard" which are commonly related to ISO stuff.

You won't want to implement the same standard for everything as you should consider the aspects of the projects from their conception.


upvoted 2 times

🗳️ 👤 **k4d4v4r** 3 years, 1 month ago

I agree with A.

B is factible but not the first thing you would do.

upvoted 1 times

  **837vq3** 3 years, 1 month ago



Selected Answer: A

Perhaps "A"?

Privacy by Design principle includes:

1. Proactive, not reactive – preventative, not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Fully functionality
5. End-to-end security – full life cycle protection
6. Visibility and transparency
7. Respect for user privacy

upvoted 3 times

  **k4d4v4r** 3 years, 2 months ago

Why B ?

upvoted 2 times

When releasing aggregates, what must be performed to magnitude data to ensure privacy?

- A. Value swapping.
- B. Noise addition.
- C. Basic rounding.
- D. Top coding.

Suggested Answer: B

Reference:

<https://academic.oup.com/idpl/article/8/1/29/4930711>

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Noise addition.

upvoted 2 times

🗨️ 👤 **837vq3** 3 years, 3 months ago

One way to prevent reverse engineering is to "blur" the data points by using noise addition through differential privacy. The goal is to ensure that the aggregated data is still useful, while also making it nonspecific enough to avoid revealing the underlying identifiers.

upvoted 1 times

What term describes two re-identifiable data sets that both come from the same unidentified individual?

- A. Pseudonymous data.
- B. Anonymous data.
- C. Aggregated data.
- D. Imprecise data.

Suggested Answer: A

Community vote distribution

A (86%) 14%

🗳️ **forest_gump33** 3 months, 3 weeks ago

Selected Answer: C

If it is re-identifiable, it is not anonymous.
upvoted 1 times

🗳️ **z80r** 1 year ago

Selected Answer: A

A is correct
upvoted 1 times

🗳️ **Magim1920** 1 year, 7 months ago

Selected Answer: A

Anonymity is the polar opposite of re-identifiability
upvoted 1 times

🗳️ **187san** 2 years, 1 month ago

Selected Answer: A

A is the answer
upvoted 2 times

🗳️ **187san** 2 years, 1 month ago

Selected Answer: A

A for sure required by GDPR also
upvoted 1 times

🗳️ **k4d4v4r** 2 years, 1 month ago

There this example for A also:

HIPAA also provides a specific example of pseudonymity. A de-identified dataset may include:

A code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that: (1) the code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and (2) the covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

upvoted 1 times

🗳️ **k4d4v4r** 2 years, 1 month ago

Selected Answer: A

<https://en.wikipedia.org/wiki/Pseudonymization>
upvoted 1 times

🗳️ **837vq3** 2 years, 1 month ago

But the wiki says "GDPR Data Protection by Design and by Default principles as embodied in pseudonymization require protection of both direct and indirect identifiers so that personal data is NOT cross-referenceable (or re-identifiable) via the "Mosaic Effect"
upvoted 1 times

🗳️ **837vq3** 2 years, 3 months ago

I think its "d". "Labels: Labels are characteristics that point to an individual. These can be precise, as in a name, or imprecise, such as with an attribute, depending on the context. Labeling people based on an attribute, instead of by name, may make them easier to identify in context. For instance, a man in a business suit may not be identifiable within a large corporate office, but the same man in a business suit may be easily identifiable among sunbathers on a beach."

upvoted 1 times

Which of the following most embodies the principle of Data Protection by Default?

- A. A messaging app for high school students that uses HTTPS to communicate with the server.
- B. An electronic teddy bear with built-in voice recognition that only responds to its owner's voice.
- C. An internet forum for victims of domestic violence that allows anonymous posts without registration.
- D. A website that has an opt-in form for marketing emails when registering to download a whitepaper.

Suggested Answer: C

Community vote distribution

C (75%)

A (25%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. An internet forum for victims of domestic violence that allows anonymous posts without registration.

Data Protection by Default means that privacy and data protection measures are integrated into the design and operation of a system or process from the outset. Allowing anonymous posts without requiring registration aligns with this principle by minimizing the amount of personal data collected and reducing the risk of identifying individuals, thus enhancing their privacy and security by default.

upvoted 1 times

🗨️ 👤 **Stants** 11 months, 1 week ago

You've provided a detailed and thoughtful analysis. I agree with your conclusion that the principle of Data Protection by Default is most embodied by Option B: An electronic teddy bear with built-in voice recognition that only responds to its owner's voice.

This option minimizes data collection and processing to the bare minimum needed for its intended function, demonstrating a stronger alignment with Data Protection by Default compared to the other options. It aligns with the purpose of the product and ensures that only necessary data (the owner's voice) is collected and processed.

Your explanations of the other options are also accurate. Allowing anonymous posts (Option C), using HTTPS in a messaging app (Option A), and having an opt-in for marketing emails (Option D) are all important components of data protection, but they do not directly embody the principle of Data Protection by Default.

upvoted 1 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: C

Answer is c. Data mitigation by allowing anonymous post

upvoted 1 times

🗨️ 👤 **z80r** 2 years ago

Selected Answer: C

Imho is C

upvoted 1 times

🗨️ 👤 **Magim1920** 2 years, 7 months ago

Selected Answer: A

D is privacy by default, not data protection, and so is C. B is vague, but between B and A, A seems the stronger answer and clearly constitutes data protection by default, by opting to use the more secure HTTPS over HTTP

upvoted 1 times

Aadhaar is a unique-identity number of 12 digits issued to all Indian residents based on their biometric and demographic data. The data is collected by the Unique Identification Authority of India. The Aadhaar database contains the Aadhaar number, name, date of birth, gender and address of over 1 billion individuals.

Which of the following datasets derived from that data would be considered the most de-identified?

- A. A count of the years of birth and hash of the person's gender.
- B. A count of the month of birth and hash of the person's first name.
- C. A count of the day of birth and hash of the person's first initial of their first name.
- D. Account of the century of birth and hash of the last 3 digits of the person's Aadhaar number.

Suggested Answer: C

Community vote distribution

D (67%)

A (33%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. A count of the century of birth and hash of the last 3 digits of the person's Aadhaar number provides a broader de-identification strategy. The count of the century of birth is less specific, and hashing the last 3 digits of the Aadhaar number adds an additional layer of obscurity. Together, these methods provide better protection against re-identification compared to the other options.

Example Dataset Summary:

A: Year 1980 - Count 500; Gender (hashed) 5f4dcc3b5aa765d61d8327deb882cf99

B: January - Count 300; First initial "J" (hashed) 5f4dcc3b5aa765d61d8327deb882cf99

C: 1st - Count 50; First initial "J" (hashed) 5f4dcc3b5aa765d61d8327deb882cf99

D: 2000s - Count 1,000; Last 3 digits (hashed) a9d9c3ef8f83e8c1c8bcb373e1d81799

upvoted 2 times

🗨️ 👤 **Stants** 11 months, 2 weeks ago

The correct answer is D. A count of the century of birth and hash of the last 3 digits of the person's Aadhaar number. This option provides the least amount of identifiable information. The century of birth is a very broad category, and hashing the last 3 digits of the Aadhaar number does not reveal much information about the individual. The other options provide more specific information, such as the year, month, or day of birth, and more identifiable aspects of the person's name or gender, which could potentially be used to re-identify the individual. Therefore, option D is the most de-identified dataset.

upvoted 2 times

🗨️ 👤 **haha2345** 1 year, 9 months ago

Selected Answer: A

I think is A.

Gender and count of year most de-identified.

upvoted 1 times

What has been identified as a significant privacy concern with chatbots?

- A. Most chatbot providers do not agree to code audits
- B. Chatbots can easily verify the identity of the contact.
- C. Users' conversations with chatbots are not encrypted in transit.
- D. Chatbot technology providers may be able to read chatbot conversations with users.

Suggested Answer: D

Reference:

<https://resources.infosecinstitute.com/privacy-concerns-emotional-chatbots/>

Community vote distribution

D (100%)

🗉 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Chatbot technology providers may be able to read chatbot conversations with users.

A significant privacy concern with chatbots is that the technology providers may have access to the conversations between users and the chatbot. This can lead to potential privacy issues if the data is not adequately protected or if there are concerns about how the data is used or shared. While encryption in transit is important (C), the concern about provider access (D) addresses broader privacy implications related to data handling and user confidentiality.

upvoted 2 times

What is the term for information provided to a social network by a member?

- A. Profile data.
- B. Declared data.
- C. Personal choice data.
- D. Identifier information.

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Declared data.

Declared data refers to information that users provide to a social network or other online platforms voluntarily, such as personal details entered into a profile. This contrasts with data collected passively or inferred from user behavior.

upvoted 1 times

🗨️ 👤 **Magim1920** 2 years, 7 months ago

Selected Answer: B

Definitely B, declared data.

upvoted 1 times

🗨️ 👤 **ChaBum** 2 years, 11 months ago

Selected Answer: B

Here is the definition of Declared Data from iapp: Personal information that is directly given to a social network or other website by a user.

Associated term(s): Consent

upvoted 4 times

🗨️ 👤 **Sbowo** 3 years, 1 month ago

Declared data is the answer

upvoted 2 times

What tactic does pharming use to achieve its goal?

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

Suggested Answer: C

Reference:

<https://inspiredelearning.com/blog/phishing-vs-pharming-whats-difference/>

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

The correct answer is:

A. It modifies the user's Hosts file.

Pharming typically involves redirecting users from legitimate websites to fraudulent ones by altering their DNS settings or Hosts file. This tactic manipulates the user's computer settings to redirect them to a malicious site that looks like a legitimate one, aiming to capture sensitive information or perform other malicious activities.

Options B, C, and D refer to other types of cyber threats or tactics, such as ransomware, fraudulent advertisements, or instant message scams, but they are not specifically associated with pharming.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 5 months ago

Selected Answer: A

Should be A

upvoted 1 times

🗨️ 👤 **k4d4v4r** 3 years, 2 months ago

A and C are both correct

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 2 months ago

Yes, but the question is more focused on how it is achieved - which is "A". The "C" is the outcome.

upvoted 1 times

🗨️ 👤 **ChaBum** 2 years, 11 months ago

A is not necessary correct, pharming is action of redirecting to a website controlled by the hacker. The mean to achieve that goal can be tampering with the host file of the victime computer, but it can also be DNS poisoning, or much more easier URL hijacking in a phising email

upvoted 1 times

🗨️ 👤 **sirpuzee** 3 years, 3 months ago



The correct answer is A. Pharming redirects a valid internet request to a malicious site by modifying a hosts file and there is not much individuals can do about it except try to use up to date browsers. IAPP - Privacy in Technology, page 150 of the 2014 official publication

upvoted 4 times

🗨️ 👤 **Stants** 11 months, 2 weeks ago

The correct answer is A. It modifies the user's Hosts file. Pharming is a cyber attack intended to redirect a website's traffic to another, fake site. In order to achieve this, attackers often modify the user's Hosts file, which is used to look up hostnames of sites on the internet. By changing the Hosts file, the attacker can control which site the user ends up at when they type in a particular URL, leading them to a malicious site instead of the one they intended to visit.

upvoted 2 times

  **837vq3** 3 years, 3 months ago

I think the correct answer is "A". "Pharming is the redirection of a Web site's actual or intended traffic to a malicious site. Redirection is often accomplished in one of two ways: modification of host files or by taking advantage of weaknesses in DNS services.

<https://www.techrepublic.com/blog/it-security/hosts-file-pharming-and-other-botnet-recruiting-methods/>

upvoted 4 times


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.

Suggested Answer: B

Community vote distribution

B (100%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. An increased amount of spam email in an individual's inbox.

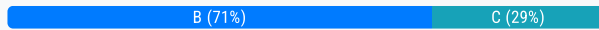
upvoted 2 times

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.

Suggested Answer: B

Community vote distribution



🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

its not clear if news site is related to wine so Answer is B
upvoted 2 times

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

Behavioral advertising does indeed use data about our browsing history and interests to target ads specifically to us. However, in the example where an ad for wine pops up on a news site, the ad placement is based on the context of the content we're viewing (news related to wine or similar topics), rather than our previous browsing behavior.

If the ad is being displayed because of your prior searches or interest in wine, then it would be considered behavioral advertising. However, if the ad is shown simply because the page content is related to wine, it's more contextual advertising. Both can be involved in different scenarios.
upvoted 1 times

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

second thought, its not clear if news site is related to wine so Answer is B
upvoted 2 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: B

The type of advertising in this scenario is Behavioral advertising.

Behavioral advertising is a type of online advertising that targets users based on their online behavior, such as their browsing history, search queries, and other actions taken online. It involves the use of cookies and other tracking technologies to collect data on users' behavior and interests, and then deliver targeted ads to them.

In this scenario, the ad for wine that popped up on the news site was likely delivered based on the user's browsing history and search queries related to wine collecting, indicating that the advertising was behaviorally targeted to the user's interests and online behavior.
upvoted 2 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: B

behavioural sorry not c
upvoted 1 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: C

Contextual advertising is a type of online advertising that displays ads that are relevant to the content of the web page being viewed. In this scenario, the news site content is likely related to wine, which triggers the display of a wine ad. The ad is not based on the user's browsing history or demographic information, but rather on the context of the web page being viewed
upvoted 1 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

Contextual
upvoted 1 times

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.

Suggested Answer: C

Reference:

https://en.wikipedia.org/wiki/Do_Not_Track

Community vote distribution

C (100%)

🗉 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. There is a lack of consensus about what the DNT header should mean.

The Do Not Track (DNT) header has faced challenges in widespread adoption primarily due to the lack of a universal agreement on what DNT should entail and how it should be implemented. Different companies and stakeholders have varying interpretations of DNT, leading to inconsistencies in how it is acknowledged and applied.

upvoted 1 times

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

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

Suggested Answer: A

Community vote distribution

A (100%)

  **k4d4v4r** Highly Voted 3 years, 1 month ago

Selected Answer: A

You basically can't login without the 1st party ones
upvoted 6 times

  **Ssourav** Most Recent 5 months, 3 weeks ago

Selected Answer: A

A. The available tools to block tracking would break most sites' functionality.

First-party web tracking is difficult to prevent because blocking these trackers often involves preventing scripts or cookies from loading, which can break or degrade the functionality of many websites. Many sites rely on first-party cookies and scripts for essential features, such as user authentication, personalization, and maintaining session states.



upvoted 2 times

  **Magim1920** 2 years, 7 months ago

Selected Answer: A

Most browsers DO support automatic blocking. They also include options to add exceptions, because doing so ever so often breaks site functionality. Answer should be A.

upvoted 3 times

  **Sbowo** 3 years, 1 month ago

I think the answer is C

upvoted 1 times

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.

Suggested Answer: C

Reference:

[https://books.google.com.pk/books?id=0aXise4B-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=ACfU3U0bT0eOfPfcOq_Y95SZs6imKKilug&hl=en&sa=X&ved=2ahUKEwjscDHpcbnAhUJuRoKHU5iC9cQ6AEwCnoECAkQAQ#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](https://books.google.com.pk/books?id=0aXise4B-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=ACfU3U0bT0eOfPfcOq_Y95SZs6imKKilug&hl=en&sa=X&ved=2ahUKEwjscDHpcbnAhUJuRoKHU5iC9cQ6AEwCnoECAkQAQ#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)

Community vote distribution

C (100%)

🗉 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

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

During a TLS (Transport Layer Security) session, after the web browser generates a random PremasterSecret, it encrypts this PremasterSecret using the server's public key. This encrypted PremasterSecret is then sent to the server. The server, which possesses the corresponding private key, decrypts the PremasterSecret. Both the client and the server use the PremasterSecret, along with additional data, to generate the session keys that will be used for encrypting the rest of the session's data.

upvoted 1 times


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.

Suggested Answer: C

Community vote distribution

C (100%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. The ability to restrict data access to employees and contractors.

upvoted 2 times

SCENARIO -

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells online through retail sites designated for industries and demographics, sites such as `My Cool Ride` for automobile-related products or `Zoomer` for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third-party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as `Under the Sun.` The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

If you are asked to advise on privacy concerns regarding paid advertisements, which is the most important aspect to cover?

- A. Unseen web beacons that combine information on multiple users.
- B. Latent keys that trigger malware when an advertisement is selected.
- C. Personal information collected by cookies linked to the advertising network.
- D. Sensitive information from Structured Query Language (SQL) commands that may be exposed.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. Personal information collected by cookies linked to the advertising network.

Paid advertisements often involve tracking users through cookies set by advertising networks. These cookies can collect personal information about users' browsing habits, preferences, and behavior, which raises significant privacy concerns. Ensuring that users are aware of and can control how their data is collected and used by these cookies is crucial for maintaining privacy.

upvoted 1 times

SCENARIO -

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells online through retail sites designated for industries and demographics, sites such as `My Cool Ride` for automobile-related products or `Zoomer` for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third-party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as `Under the Sun.` The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

What technology is under consideration in the first project in this scenario?

- A. Server driven controls.
- B. Cloud computing
- C. Data on demand
- D. MAC filtering

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Cloud computing

The project involves using third-party servers to provide company data and approved applications to employees, which aligns with cloud computing. Cloud computing involves delivering computing services over the internet, including storage, processing power, and applications, which fits the described initiative for unifying the company's culture through centralized data management and application access.

upvoted 1 times

🗨️ 👤 **steven2xx** 1 year, 8 months ago

Selected Answer: B

🗨️🗨️🗨️🗨️B

upvoted 1 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

Selected Answer: B



B.. Cloud computing

upvoted 2 times

🗨️ 👤 **Ame123456789** 1 year, 10 months ago



I would agree its cloud computing too.

upvoted 2 times

  **187san** 3 years, 1 month ago

B is the answer

upvoted 3 times

  **k4d4v4r** 3 years, 2 months ago

Why not B?

upvoted 3 times

SCENARIO -

You have just been hired by Ancillary.com, a seller of accessories for everything under the sun, including waterproof stickers for pool floats and decorative bands and cases for sunglasses. The company sells cell phone cases, e-cigarette cases, wine spouts, hanging air fresheners for homes and automobiles, book ends, kitchen implements, visors and shields for computer screens, passport holders, gardening tools and lawn ornaments, and catalogs full of health and beauty products. The list seems endless. As the CEO likes to say, Ancillary offers, without doubt, the widest assortment of low-price consumer products from a single company anywhere.

Ancillary's operations are similarly diverse. The company originated with a team of sales consultants selling home and beauty products at small parties in the homes of customers, and this base business is still thriving. However, the company now sells online through retail sites designated for industries and demographics, sites such as `My Cool Ride` for automobile-related products or `Zoomer` for gear aimed toward young adults. The company organization includes a plethora of divisions, units and outrigger operations, as Ancillary has been built along a decentered model rewarding individual initiative and flexibility, while also acquiring key assets. The retail sites seem to all function differently, and you wonder about their compliance with regulations and industry standards. Providing tech support to these sites is also a challenge, partly due to a variety of logins and authentication protocols.

You have been asked to lead three important new projects at Ancillary:

The first is the personal data management and security component of a multi-faceted initiative to unify the company's culture. For this project, you are considering using a series of third-party servers to provide company data and approved applications to employees.

The second project involves providing point of sales technology for the home sales force, allowing them to move beyond paper checks and manual credit card imprinting.

Finally, you are charged with developing privacy protections for a single web store housing all the company's product lines as well as products from affiliates. This new omnibus site will be known, aptly, as `Under the Sun.` The Director of Marketing wants the site not only to sell Ancillary's products, but to link to additional products from other retailers through paid advertisements. You need to brief the executive team of security concerns posed by this approach.

Which should be used to allow the home sales force to accept payments using smartphones?

- A. Field transfer protocol.
- B. Cross-current translation.
- C. Near-field communication
- D. Radio Frequency Identification

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. Near-field communication (NFC)

NFC enables smartphones and other devices to communicate and exchange data over short distances (typically a few centimeters), making it ideal for contactless payment systems. It allows for secure and convenient transactions using mobile payment apps or digital wallets.

upvoted 1 times

What is the best way to protect privacy on a geographic information system?

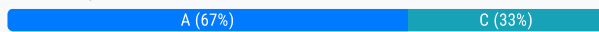
- A. Limiting the data provided to the system.
- B. Using a wireless encryption protocol.
- C. Scrambling location information.
- D. Using a firewall.

Suggested Answer: A

Reference:

https://www.researchgate.net/publication/2873114_Protecting_Personal_Privacy_in_Using_Geographic_Information_Systems

Community vote distribution



🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Limiting the data provided to the system.

By limiting the amount of sensitive or personal data provided to the GIS, you reduce the risk of privacy breaches. This involves only including necessary data and minimizing the granularity of location information to prevent the system from capturing or revealing more personal details than needed.

C. Scrambling location information: While this might provide some level of privacy, it may not be as effective as limiting the data in the first place and can complicate the use of GIS data.

upvoted 2 times

🗨️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: C

This method involves obfuscating or altering location data to prevent easy identification.

Techniques include adding noise, aggregating data, or using differential privacy.

Scrambling enhances privacy while maintaining data utility.

upvoted 1 times

🗨️ 👤 **Stants** 11 months, 2 weeks ago

The correct answer is C. Scrambling location information. Geographic Information Systems (GIS) often deal with sensitive location data.

Scrambling, or obfuscating, this data can help protect individual privacy. This could involve techniques like "geo-masking" or "geo-hashing" which alter the precise location data to protect privacy while still providing useful information for spatial analysis. Other options like limiting data, using encryption, or firewalls can also contribute to security, but they do not directly address the privacy concerns associated with the specific nature of geographic data.

upvoted 1 times

In the realm of artificial intelligence, how has deep learning enabled greater implementation of machine learning?

- A. By using hand-coded classifiers like edge detection filters so that a program can identify where an object starts and stops.
- B. By increasing the size of neural networks and running massive amounts of data through the network to train it.
- C. By using algorithmic approaches such as decision tree learning and inductive logic programming.
- D. By hand coding software routines with a specific set of instructions to accomplish a task.

Suggested Answer: B

Reference:

<https://towardsdatascience.com/notes-on-artificial-intelligence-ai-machine-learning-ml-and-deep-learning-dl-for-56e51a2071c2>

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. By increasing the size of neural networks and running massive amounts of data through the network to train it.

Deep learning involves using large neural networks with many layers (hence "deep") to analyze and learn from vast amounts of data. This approach allows models to automatically learn and extract complex features from data without the need for manual feature engineering, which significantly enhances the capabilities and performance of machine learning systems.

upvoted 1 times

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

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

Suggested Answer: B

Community vote distribution

B (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. An insurance company raises a person's rates based on driving habits gathered from a connected car.

IoT devices, such as connected cars, collect and transmit personal data, including driving habits. This data can be used by third parties, such as insurance companies, to make decisions about pricing or coverage, potentially leading to privacy concerns if the data is used in ways that the individual did not anticipate or consent to.

upvoted 1 times

🗳️ 👤 **Ame123456789** 1 year, 10 months ago

if B is correct, so is D. Both are cases whereby the original intent (B - safety, and D - water consumption monitoring) have been abused.

upvoted 1 times

🗳️ 👤 **z80r** 2 years ago

I think B is correct (privacy implications)

upvoted 1 times

🗳️ 👤 **vicks888** 3 years, 1 month ago

2. is Vehicular Automation.

upvoted 1 times

🗳️ 👤 **k4d4v4r** 3 years, 2 months ago

Power grid is OT (Operational technology)

Connected cars are IoT (Internet of things or things connected to the internet)

upvoted 2 times

🗳️ 👤 **837vq3** 3 years, 3 months ago

infiltrating a power grid is causing a major blackout - there is no risk to privacy mentioned. This is affecting the availability of the system. What are the privacy implication?

upvoted 1 times

🗳️ 👤 **sirpuzee** 3 years, 3 months ago

The correct answer is A. Anything that is connected to the Internet or the cellular phone network can possibly be hacked by an intruder. IAPP Privacy in Technology publication, page 202.

upvoted 1 times

🗳️ 👤 **837vq3** 3 years, 2 months ago

Isn't the same true for a sensor in the car?

upvoted 1 times

🗳️ 👤 **pipzz** 3 years, 4 months ago

The answer is A.

upvoted 2 times

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

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

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. By installing a roving bug on the phone.

A "roving bug" refers to malicious software or spyware installed on the phone that allows the hacker to remotely access the device's camera and microphone for surveillance purposes. This type of malware can be delivered through various methods, such as phishing attacks or malicious apps.

upvoted 2 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

A hacker can gain control of a smartphone to perform remote audio and video surveillance by installing a roving bug on the phone. A roving bug is a software application that can be installed on a mobile device without the user's knowledge, which allows an attacker to activate the phone's microphone and camera and listen in on conversations and capture video footage. The attacker can remotely control the bug, turning it on and off, and even adjust the audio and video settings. This type of attack can be very difficult to detect and can compromise a user's privacy and security.

upvoted 2 times

🗨️ 👤 **Ame123456789** 1 year, 10 months ago

I've done many google searches - roving bug does not activate video recording, only voice recording .

upvoted 1 times

🗨️ 👤 **rajiabdmjd** 1 year, 10 months ago

If it can access audio then what's stopping it from accessing video ?

upvoted 1 times

🗨️ 👤 **Magim1920** 2 years, 7 months ago

Theoretically, this could be achieved by cross site scripting, because that is just the method of delivering the payload.

upvoted 1 times

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.

In a business strategy session held by senior management recently, Clean-Q invited vendors to present potential solutions to their current operational issues.

These vendors included Application developers and cloud solution providers, presenting their proposed solutions and platforms.

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

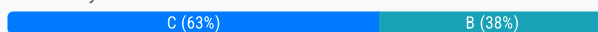
- ⇒ A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
- ⇒ A resource facing web interface that enables resources to apply and manage their assigned jobs.
- ⇒ An online payment facility for customers to pay for services.

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

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

Suggested Answer: C

Community vote distribution



🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. A provision prescribing technical and organizational controls that LeadOps must implement.

This provision ensures that LeadOps follows specific standards and practices for securing data, which is foundational for maintaining data privacy and security throughout the duration of the contract. However, combining this with other provisions such as breach notification (C) and audit rights (D) would provide a comprehensive approach to managing data protection risks.

upvoted 1 times

🗨️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: C

Clean Q is the Controller , Lead OPS operator

upvoted 1 times

🗨️ 👤 **Ame123456789** 1 year, 10 months ago

Poor question scribing, I feel.


A. A provision that holds LeadOps liable for a data breach involving Clean-Q's information.
is probably true. Contracts is about liability and indemnities. So "liable" word is used with a different meaning.

B. A provision prescribing technical and organizational controls that LeadOps must implement.
not right - DC may not be in the position to scribe.

C. A provision that requires LeadOps to notify Clean-Q of any suspected breaches of information that involves customer or resource information managed on behalf of Clean-Q.
maybe right - the "on behalf of Clean Q" is just saying that LeadOps is managing the data on behalf. not reporting to regulator on behalf.



D. A provision that allows Clean-Q to conduct audits of LeadOps' information processing and information security environment, at LeadOps' cost and at any time that Clean-Q requires.
in reality, this clause is common, but "not any time that Clean Q requires" - impractical.

So C is likely to be the right answer
upvoted 1 times



  **pipzz** 2 years, 6 months ago

Selected Answer: C

Best answer. The GDPR requires a processor to notify a controller if it becomes aware of a breach of personal data it is processing on behalf of the controller. The governing legal document may provide for a stricter notification requirement, including notification if the processor even merely "suspects" a breach has occurred.
upvoted 1 times

  **Magim1920** 2 years, 7 months ago

It's almost as if the question is wrong and should read "What is NOT a contractual clause...". All of these are commonly found in SSCs in European Union countries, except A - you cannot outsource your liability as data controller to a processor.
upvoted 2 times

  **ChaBum** 2 years, 11 months ago



Selected Answer: B

B, the TOMs Technical and Organisational Measures (GDPR Art 32 & Recital 78),
upvoted 2 times


  **k4d4v4r** 3 years, 1 month ago

Selected Answer: C



C is the best answer.
Never saw a D situation in real life scenarios.
upvoted 3 times

  **ChaBum** 2 years, 11 months ago

There is no reason to inform an external party about a SUSPECTED breach
upvoted 1 times

  **837vq3** 3 years, 3 months ago

The part that I do not like in "D" is this: "at LeadOps' cost and at any time that Clean-Q requires". As far as I know, audits are not performed at the expense of the vendor. If the client wants to audit a vendor, the client pays for it, correct?
upvoted 2 times

  **ChaBum** 2 years, 11 months ago

It could be part of the contract to have the vendor pass through audits on regular basis. But those audits are conducted by third party company and not the client. If a client want to audit a vendor, the vendor will normally charge the client for the resources provided to conduct the audit.
What I find non-realistic is the "at any time that Clean-Q requires", the audit should happen at a time which is convenient for both parties.
upvoted 1 times

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.

In a business strategy session held by senior management recently, Clean-Q invited vendors to present potential solutions to their current operational issues.

These vendors included Application developers and cloud 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.

Suggested Answer: D

Community vote distribution

D (100%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Involve the Information Security team to understand in more detail the types of services and solutions LeadOps is proposing.
upvoted 1 times

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.

In a business strategy session held by senior management recently, Clean-Q invited vendors to present potential solutions to their current operational issues.

These vendors included Application developers and cloud solution providers, presenting their proposed solutions and platforms.

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

- ⇒ A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
- ⇒ A resource facing web interface that enables resources to apply and manage their assigned jobs.
- ⇒ An online payment facility for customers to pay for services.

Which question would you most likely ask to gain more insight about LeadOps and provide practical privacy recommendations?

- A. What is LeadOps' annual turnover?
- B. How big is LeadOps' employee base?
- C. Where are LeadOps' operations and hosting services located?
- D. Does LeadOps practice agile development and maintenance of their system?

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

To gain more insight about LeadOps and provide practical privacy recommendations, the most relevant question would be:

C. Where are LeadOps' operations and hosting services located?

upvoted 1 times

🗨️ **pipzz** 2 years, 6 months ago

Selected Answer: C

Location is crucial to know. There are legal requirements with transfers of personal data to third countries or international organisations, which would need to be built into the agreement.

upvoted 3 times

🗨️ **187san** 3 years, 1 month ago

C is the answer

upvoted 3 times

🗨️ **837vq3** 3 years, 3 months ago

"C" is a better choice. What does agile development have to do with privacy?
upvoted 4 times

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.

In a business strategy session held by senior management recently, Clean-Q invited vendors to present potential solutions to their current operational issues.

These vendors included Application developers and cloud solution providers, presenting their proposed solutions and platforms.

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

- ⇒ A customer facing web interface that enables customers to register, manage and submit cleaning service requests online.
- ⇒ A resource facing web interface that enables resources to apply and manage their assigned jobs.
- ⇒ An online payment facility for customers to pay for services.


What is a key consideration for assessing external service providers like LeadOps, which will conduct personal information processing operations on Clean-Q's behalf?

- A. Understanding LeadOps' costing model.
- B. Establishing a relationship with the Managing Director of LeadOps.
- C. Recognizing the value of LeadOps' website holding a verified security certificate.
- D. Obtaining knowledge of LeadOps' information handling practices and information security environment.

Suggested Answer: D

Community vote distribution

D (100%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Obtaining knowledge of LeadOps' information handling practices and information security environment.
upvoted 1 times


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

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

Suggested Answer: B

Community vote distribution

B (100%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Ensure surveillance is discreet so employees do not alter their behavior.

upvoted 1 times

A sensitive biometrics authentication system is particularly susceptible to?

- A. False positives.
- B. False negatives.
- C. Slow recognition speeds.
- D. Theft of finely individualized personal data.

Suggested Answer: B

Reference:

<https://link.springer.com/article/10.1007/s41403-017-0026-8>

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Theft of finely individualized personal data.

Here's why:

Sensitive Personal Data: Biometric systems use unique personal characteristics, such as fingerprints or facial features, to authenticate users. If these biometric data are stolen, they are very difficult to change compared to passwords or other credentials. The theft of biometric data poses a significant privacy risk because such data is tied directly to the individual and can be used for various forms of identity theft or fraud.

upvoted 1 times

Which is the most accurate type of biometrics?

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

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. DNA

Here's why:

DNA: DNA biometrics is considered the most accurate form of biometric identification because it relies on the unique genetic code of an individual. Each person's DNA is unique (except for identical twins), making it highly reliable for identification. DNA analysis can provide very high accuracy, though it's also complex and costly.

upvoted 1 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: A

I think it's A

upvoted 1 times

🗳️ 👤 **samaja** 2 years, 9 months ago

Selected Answer: A

DNA is the most accurate biometric

upvoted 1 times

🗳️ 👤 **187san** 3 years, 1 month ago

Selected Answer: A

A

ITS A

upvoted 1 times

🗳️ 👤 **k4d4v4r** 3 years, 2 months ago

DNA might be the best answer

upvoted 3 times

🗳️ 👤 **837vq3** 3 years, 3 months ago

Not sure how correct the voiceprint is. The provided link does not mention voiceprint as being the most accurate. Any suggestions?

upvoted 1 times



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.

Suggested Answer: B

Community vote distribution

B (100%)

  **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. They can see all unencrypted data that crosses the system.

Here's an explanation:

B. They can see all unencrypted data that crosses the system: Wireless technology providers, such as those managing Wi-Fi or cellular networks, can potentially access unencrypted data that passes through their systems. This is because unencrypted data is transmitted in a form that can be intercepted and viewed by those operating the network.

upvoted 2 times

What distinguishes a "smart" device?

- A. It can perform multiple data functions simultaneously.
- B. It is programmable by a user without specialized training.
- C. It can reapply access controls stored in its internal memory.
- D. It augments its intelligence with information from the internet.

Suggested Answer: D

Reference:

<https://towardsdatascience.com/what-is-a-smart-device-the-key-concept-of-the-internet-of-things-52da69f6f91b>

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. It augments its intelligence with information from the internet.

Explanation: A "smart" device typically leverages internet connectivity to enhance its functionality and intelligence by accessing and processing information online.

upvoted 2 times

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

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

Suggested Answer: B

Reference:

<https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-report-summary.pdf>

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. To protect sensitive data while maintaining its utility.

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 2 months ago

(PET) are technologies that embody fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individuals. PETs allow online users to protect the privacy of their personally identifiable information (PII) provided to and handled by services or applications. PETs use techniques to minimize possession of personal data without losing the functionality of an information system. Generally speaking, PETs can be categorized as hard and soft privacy technologies.

upvoted 1 times

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.

Suggested Answer: C

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Modification of data is an aspect of privacy; unauthorized use, disclosure, and damage or loss of data are aspects of security.

upvoted 1 times

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.

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. A North American company servicing customers in South Africa that uses a cloud storage system made by a European company.

Explanation: GDPR applies to entities processing personal data of individuals in the EU, regardless of where the entity itself is based. Since the North American company primarily services South African customers and does not handle EU residents' data, it is not required to comply with GDPR.

upvoted 1 times

🗨️ 👤 **z80r** 2 years ago

Selected Answer: D

D is the right answer

upvoted 2 times

🗨️ 👤 **187san** 3 years, 1 month ago

D

same question is there in CIPP EU

upvoted 3 times

🗨️ 👤 **flyingrain777** 3 years, 2 months ago

I concur.

upvoted 4 times

🗨️ 👤 **k4d4v4r** 3 years, 2 months ago

D. is correct. No way it's C as it servers european people

upvoted 4 times

SCENARIO -

WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider

AmaZure, which provides SQL Databases and Artificial Intelligence services to WebTracker. The roles and responsibilities between the two companies have been formalized in a standard contract, which includes allocating the role of data controller to WebTracker.

The CEO of WebTracker, Mr. Bond, would like to assess the effectiveness of AmaZure's privacy controls, and he recently decided to hire you as an independent auditor. The scope of the engagement is limited only to the marketing services provided by WebTracker, you will not be evaluating any internal data processing activity, such as HR or Payroll.

This ad-hoc audit was triggered due to a future partnership between WebTracker and SmartHome " a partnership that will not require any data sharing.

SmartHome is based in the USA, and most recently has dedicated substantial resources to developing smart refrigerators that can suggest the recommended daily calorie intake based on DNA information. This and other personal data is collected by WebTracker.

To get an idea of the scope of work involved, you have decided to start reviewing the company's documentation and interviewing key staff to understand potential privacy risks.

The results of this initial work include the following notes:

- ⇒ There are several typos in the current privacy notice of WebTracker, and you were not able to find the privacy notice for SmartHome.
- ⇒ You were unable to identify all the sub-processors working for SmartHome. No subcontractor is indicated in the cloud agreement with AmaZure, which is responsible for the support and maintenance of the cloud infrastructure.
- ⇒ There are data flows representing personal data being collected from the internal employees of WebTracker, including an interface from the HR system.
- ⇒ Part of the DNA data collected by WebTracker was from employees, as this was a prototype approved by the CEO of WebTracker.
- ⇒ All the WebTracker and SmartHome customers are based in USA and Canada.

Based on the initial assessment and review of the available data flows, which of the following would be the most important privacy risk you should investigate first?

- A. Verify that WebTracker's HR and Payroll systems implement the current privacy notice (after the typos are fixed).
- B. Review the list of subcontractors employed by AmaZure and ensure these are included in the formal agreement with WebTracker.
- C. Evaluate and review the basis for processing employees' personal data in the context of the prototype created by WebTracker and approved by the CEO.
- D. Confirm whether the data transfer from London to the USA has been fully approved by AmaZure and the appropriate institutions in the USA and the European Union.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. Evaluate and review the basis for processing employees' personal data in the context of the prototype created by WebTracker and approved by the CEO.

Explanation: Ensuring that the processing of employees' personal data, particularly sensitive data like DNA information, is justified and compliant with privacy regulations is crucial. This review addresses both the legal basis for processing and the potential risks associated with handling such data.

upvoted 2 times

SCENARIO -

WebTracker Limited is a cloud-based online marketing service located in London. Last year, WebTracker migrated its IT infrastructure to the cloud provider

AmaZure, which provides SQL Databases and Artificial Intelligence services to WebTracker. The roles and responsibilities between the two companies have been formalized in a standard contract, which includes allocating the role of data controller to WebTracker.

The CEO of WebTracker, Mr. Bond, would like to assess the effectiveness of AmaZure's privacy controls, and he recently decided to hire you as an independent auditor. The scope of the engagement is limited only to the marketing services provided by WebTracker, you will not be evaluating any internal data processing activity, such as HR or Payroll.

This ad-hoc audit was triggered due to a future partnership between WebTracker and SmartHome " a partnership that will not require any data sharing.

SmartHome is based in the USA, and most recently has dedicated substantial resources to developing smart refrigerators that can suggest the recommended daily calorie intake based on DNA information. This and other personal data is collected by WebTracker.

To get an idea of the scope of work involved, you have decided to start reviewing the company's documentation and interviewing key staff to understand potential privacy risks.

The results of this initial work include the following notes:

- ⇒ There are several typos in the current privacy notice of WebTracker, and you were not able to find the privacy notice for SmartHome.
- ⇒ You were unable to identify all the sub-processors working for SmartHome. No subcontractor is indicated in the cloud agreement with AmaZure, which is responsible for the support and maintenance of the cloud infrastructure.
- ⇒ There are data flows representing personal data being collected from the internal employees of WebTracker, including an interface from the HR system.
- ⇒ Part of the DNA data collected by WebTracker was from employees, as this was a prototype approved by the CEO of WebTracker.
- ⇒ All the WebTracker and SmartHome customers are based in USA and Canada.

Which of the following issues is most likely to require an investigation by the Chief Privacy Officer (CPO) of WebTracker?

- A. Data flows use encryption for data at rest, as defined by the IT manager.
- B. AmaZure sends newsletter to WebTracker customers, as approved by the Marketing Manager.
- C. Employees' personal data are being stored in a cloud HR system, as approved by the HR Manager.
- D. File Integrity Monitoring is being deployed in SQL servers, as indicated by the IT Architect Manager.

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. AmaZure sends newsletters to WebTracker customers, as approved by the Marketing Manager.

Explanation: The Chief Privacy Officer (CPO) should investigate this issue to ensure that sending newsletters complies with privacy regulations, such as obtaining proper consent and managing customer data appropriately.

upvoted 2 times

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.

Suggested Answer: D

Community vote distribution

B (50%)

C (50%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. New Company should manage stakeholder expectations for privacy even when the stakeholders' data is not held by New Company.


Managing stakeholder expectations for privacy is crucial, regardless of whether New Company directly holds the data or not. This helps maintain trust and transparency.

upvoted 1 times

 **Sharon2000** 8 months, 1 week ago

I think it is B


upvoted 1 times

 **Sbowo** 3 years, 1 month ago

Selected Answer: C


I think C is the saver answer adhering legal compliance

upvoted 1 times

 **187san** 3 years, 1 month ago

B is the answer

upvoted 3 times

 **837vq3** 3 years, 2 months ago

I think the correct answer is "B". The New Company is due to the merger of the other two companies and should be responsible for all of the data regardless of which subsidiary it belong to
upvoted 4 times

SCENARIO -

Tom looked forward to starting his new position with a U.S.-based automobile leasing company (New Company), now operating in 32 states. New Company was recently formed through the merger of two prominent players, one from the eastern region (East Company) and one from the western region (West Company).

Tom, a Certified Information Privacy Technologist (CIPT), is New Company's first Information Privacy and Security Officer. He met today with Dick from East

Company, and Harry, from West Company. Dick and Harry are veteran senior information privacy and security professionals at their respective companies, and continue to lead the east and west divisions of New Company. The purpose of the meeting was to conduct a SWOT (strengths/weaknesses/opportunities/threats) analysis for New Company. Their SWOT analysis conclusions are summarized below.

Dick was enthusiastic about an opportunity for the New Company to reduce costs and increase computing power and flexibility through cloud services. East

Company had been contemplating moving to the cloud, but West Company already had a vendor that was providing it with software-as-a-service (SaaS). Dick was looking forward to extending this service to the eastern region. Harry noted that this was a threat as well, because West Company had to rely on the third party to protect its data.

Tom mentioned that neither of the legacy companies had sufficient data storage space to meet the projected growth of New Company, which he saw as a weakness. Tom stated that one of the team's first projects would be to construct a consolidated New Company data warehouse. Tom would personally lead this project and would be held accountable if information was modified during transmission to or during storage in the new data warehouse.

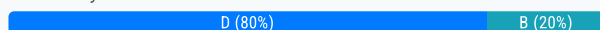
Tom, Dick and Harry agreed that employee network access could be considered both a strength and a weakness. East Company and West Company had strong performance records in this regard; both had robust network access controls that were working as designed. However, during a projected year-long transition period, New Company employees would need to be able to connect to a New Company network while retaining access to the East Company and West Company networks.

When employees are working remotely, they usually connect to a Wi-Fi network. What should Harry advise for maintaining company security in this situation?

- A. Hiding wireless service set identifiers (SSID).
- B. Retaining the password assigned by the network.
- C. Employing Wired Equivalent Privacy (WEP) encryption.
- D. Using tokens sent through HTTP sites to verify user identity.

Suggested Answer: A

Community vote distribution



hele_meneer 3 weeks, 3 days ago

Selected Answer: D

The best answer is none of the above, as none of the provided options aligns with strong security practices for remote employees connecting to Wi-Fi networks. However, I'll explain why each option is problematic and suggest a more appropriate approach:

upvoted 1 times

Ssourav 5 months, 3 weeks ago

Selected Answer: B

B. Retaining the password assigned by the network.

Ensuring the password is secure and regularly updated helps protect the network from unauthorized access, maintaining company security.

A. Hiding wireless service set identifiers (SSID) is not a strong security measure on its own because it only hides the network name but does not prevent unauthorized access. Determined attackers can still discover hidden SSIDs.


D. Using tokens sent through HTTP sites is insecure because HTTP does not encrypt data, making it vulnerable to interception. Secure methods, like HTTPS, are recommended for transmitting sensitive information.

upvoted 1 times

Sharon2000 8 months, 1 week ago

Not D, as it is HTTP and not HTTPS ?

upvoted 1 times

 **ME79** 1 year, 9 months ago

Selected Answer: D

If the employee is working remotely, they are typically not the administrator of the wireless network (unless it is their home network). Therefore hiding the SSID can not be an option.

The most correct option would be to use a VPN, however that is not listed as an option. Therefore, choice D, using tokens implies MFA, which is something that a company can set up to validate the identity of an employee that is trying to connect.

upvoted 3 times

SCENARIO -

Looking back at your first two years as the Director of Personal Information Protection and Compliance for the Berry Country Regional Medical Center in Thorn

Bay, Ontario, Canada, you see a parade of accomplishments, from developing state-of-the-art simulation based training for employees on privacy protection to establishing an interactive medical records system that is accessible by patients as well as by the medical personnel. Now, however, a question you have put off looms large: how do we manage all the data-not only records produced recently, but those still on hand from years ago? A data flow diagram generated last year shows multiple servers, databases, and work stations, many of which hold files that have not yet been incorporated into the new records system. While most of this data is encrypted, its persistence may pose security and compliance concerns. The situation is further complicated by several long-term studies being conducted by the medical staff using patient information. Having recently reviewed the major Canadian privacy regulations, you want to make certain that the medical center is observing them.

You also recall a recent visit to the Records Storage Section, often termed `The Dungeon` in the basement of the old hospital next to the modern facility, where you noticed a multitude of paper records. Some of these were in crates marked by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. The back shelves of the section housed data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the dungeon, you noticed just ahead of you a small man in a lab coat who you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.

Which regulation most likely applies to the data stored by Berry Country Regional Medical Center?

- A. Personal Information Protection and Electronic Documents Act
- B. Health Insurance Portability and Accountability Act
- C. The Health Records Act 2001
- D. The European Union Directive 95/46/EC

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA is the Canadian privacy law that applies to personal information collected, used, or disclosed in the course of commercial activities, which includes medical records and patient information in Canada.

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 3 months ago

Update: The correct answer is "A" . "PIPEDA" is in Canada and the company in the question is in Canada.

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 3 months ago

Why not "B" " Health Insurance Portability and Accountability Act"?

upvoted 1 times

🗨️ 👤 **ChaBum** 2 years, 11 months ago

Berry Country Regional Medical Center is located in Canada

upvoted 1 times

SCENARIO -

Looking back at your first two years as the Director of Personal Information Protection and Compliance for the Berry Country Regional Medical Center in Thorn

Bay, Ontario, Canada, you see a parade of accomplishments, from developing state-of-the-art simulation based training for employees on privacy protection to establishing an interactive medical records system that is accessible by patients as well as by the medical personnel. Now, however, a question you have put off looms large: how do we manage all the data—not only records produced recently, but those still on hand from years ago? A data flow diagram generated last year shows multiple servers, databases, and work stations, many of which hold files that have not yet been incorporated into the new records system. While most of this data is encrypted, its persistence may pose security and compliance concerns. The situation is further complicated by several long-term studies being conducted by the medical staff using patient information. Having recently reviewed the major Canadian privacy regulations, you want to make certain that the medical center is observing them.

You also recall a recent visit to the Records Storage Section, often termed `The Dungeon` in the basement of the old hospital next to the modern facility, where you noticed a multitude of paper records. Some of these were in crates marked by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. The back shelves of the section housed data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the dungeon, you noticed just ahead of you a small man in a lab coat who you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.


Which data lifecycle phase needs the most attention at this Ontario medical center?

- A. Retention
- B. Disclosure
- C. Collection
- D. Use

Suggested Answer: A

Community vote distribution

A (100%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Retention

Given the concerns about old, unorganized records and the need to ensure compliance with privacy regulations, managing the retention of data—ensuring that data is kept only as long as necessary and securely archived or disposed of—is critical.

upvoted 1 times

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

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Symmetric Encryption

Symmetric encryption is most appropriate for protecting patient credit card information due to its efficiency in encrypting and decrypting large volumes of data quickly and securely with the same key.

upvoted 1 times

🗨️ **k4d4v4r** 3 years, 1 month ago

Selected Answer: B

Use this as reference:

<https://security.stackexchange.com/questions/229044/symmetric-vs-asymmetric-encryption-for-backup-files-uploaded-to-cloud-storage>

upvoted 3 times

Users of a web-based email service have their accounts breached through compromised login credentials. Which possible consequences of the breach illustrate the two categories of Calo's Harm Dimensions?

- A. Financial loss and blackmail.
- B. Financial loss and solicitation.
- C. Identity theft and embarrassment.
- D. Identity theft and the leaking of information.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Trepanij** 2 months, 1 week ago

Selected Answer: C

Answer is C.

Extracts from The boundaries of privacy harms: "Objective harms can also occur when such information is used to commit a crime, such as identity theft or murder."; "The subjective category of privacy harm is the perception of unwanted observation. This category describes unwelcome mental states—anxiety, for instance, or embarrassment—that accompany the belief that one is or will be watched or monitored. "

upvoted 3 times

🗨️ 👤 **187san** 1 year, 1 month ago

C is the answer

upvoted 3 times

🗨️ 👤 **k4d4v4r** 1 year, 1 month ago

Selected Answer: C

Every other option has something that you can count, as "the amount of blackmails, solicitations and data leaked". If you can count than it's objective harm.

upvoted 3 times

🗨️ 👤 **837vq3** 1 year, 3 months ago

I think correct answer is "C". Its the only option that has both "objective" and "subjective" harm elements

upvoted 3 times

Implementation of privacy controls for compliance with the requirements of the Children's Online Privacy Protection Act (COPPA) is necessary for all the following situations EXCEPT?

- A. A virtual jigsaw puzzle game marketed for ages 5-9 displays pieces of the puzzle on a handheld screen. Once the child completes a certain level, it flashes a message about new themes released that day.
- B. An interactive toy copies a child's behavior through gestures and kid-friendly sounds. It runs on battery power and automatically connects to a base station at home to charge itself.
- C. A math tutoring service commissioned an advertisement on a bulletin board inside a charter school. The service makes it simple to reach out to tutors through a QR-code shaped like a cartoon character.
- D. A note-taking application converts hard copies of kids' class notes into audio books in seconds. It does so by using the processing power of idle server farms.

Suggested Answer: A

Community vote distribution

B (50%) A (25%) C (25%)

🗨️ **hele_meneer** 3 weeks, 3 days ago

Selected Answer: A

A and C don't collect children data

upvoted 1 times

🗨️ **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. A math tutoring service commissioned an advertisement on a bulletin board inside a charter school. The service makes it simple to reach out to tutors through a QR-code shaped like a cartoon character.

Explanation: COPPA applies to services that directly collect personal information from children under 13 online. An advertisement on a bulletin board does not involve online collection or processing of children's personal information.

upvoted 1 times

🗨️ **Stants** 11 months, 1 week ago

Option C: A math tutoring service commissioned an advertisement on a bulletin board inside a charter school. The service makes it simple to reach out to tutors through a QR-code shaped like a cartoon character.

This option describes an offline advertising method that does not involve online data collection or interaction. It simply promotes a service and provides contact information, which does not fall under the purview of COPPA.

Your explanations of the other options are also accurate. Options A, B, and D all involve online activities or services that collect or use children's data, and thus would require compliance with COPPA. Always remember that the specific requirements of COPPA can vary depending on the context and the specific needs of the users.

upvoted 1 times

🗨️ **pipzz** 2 years, 6 months ago

Selected Answer: B

B is the only one with no online connection so no data is being shared.

upvoted 2 times

Which of the following does NOT illustrate the 'respect to user privacy' principle?

- A. Implementing privacy elements within the user interface that facilitate the use of technology by any visually-challenged users.
- B. Enabling Data Subject Access Request (DSARs) that provide rights for correction, deletion, amendment and rectification of personal information.
- C. Developing a consent management self-service portal that enables the data subjects to review the details of consent provided to an organization.
- D. Filing breach notification paperwork with data protection authorities which detail the impact to data subjects.

Suggested Answer: D

Community vote distribution

D (50%)

A (50%)

🗳️ 👤 **waterdogs** 4 months, 4 weeks ago

Selected Answer: D

D. obviously
upvoted 2 times

🗳️ 👤 **moxiangnaicha** 5 months, 1 week ago

Selected Answer: A

Organizations should provide clear and easily understandable information about their data collection and usage practices. A is to facilitate "transparency" principle.
upvoted 1 times

🗳️ 👤 **moxiangnaicha** 5 months, 1 week ago

Sorry I mean A is correct, the "NOT" answer is D.
upvoted 2 times

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Implementing privacy elements within the user interface that facilitate the use of technology by any visually-challenged users.

Explanation: While this practice is important for accessibility, it does not specifically address the principle of "respect to user privacy," which focuses on how personal data is managed and protected, rather than on accessibility features.
upvoted 1 times

🗳️ 👤 **Ssourav** 5 months, 2 weeks ago

on second thought, I would go for D. Filing breach notification paperwork with data protection authorities which detail the impact to data subjects: While this is a legal obligation and important for compliance, it is more about addressing the aftermath of a privacy issue rather than proactively respecting user privacy. It does not directly illustrate respecting user privacy in the design or operation of systems.
upvoted 3 times

🗳️ 👤 **Stants** 11 months, 1 week ago

The option that does NOT illustrate the 'respect to user privacy' principle is Option A: Implementing privacy elements within the user interface that facilitate the use of technology by any visually-challenged users.

While this option is important for accessibility and inclusivity, it doesn't directly relate to privacy. It's more about making the technology usable for all individuals, regardless of their visual abilities.

The other options (B, C, and D) are all directly related to respecting user privacy. They involve giving users control over their personal data (Option B and C) and ensuring transparency about data breaches (Option D), which are key aspects of privacy. Always remember that the specific implementation of privacy protections can vary depending on the context and the specific needs of the users.

upvoted 1 times

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.

Suggested Answer: C

Reference:

<https://searchcio.techtarget.com/definition/value-sensitive-design-VSD>

Community vote distribution

B (100%)

837vq3 **Highly Voted** 3 years, 3 months ago

"B" because "Value-sensitive design is a design approach that accounts for moral and ethical values and should be considered when assessing the overall value of a design.

upvoted 8 times

hele_meneer **Most Recent** 3 weeks, 3 days ago

Selected Answer: B

B. Ethics and morality.

Explanation:

Value Sensitive Design (VSD) is an approach to designing technology that explicitly takes into account human values, including ethical considerations and moral principles. It seeks to ensure that technology aligns with societal norms and individual values while addressing potential ethical concerns during its design, development, and deployment.

Key aspects of VSD include:

Incorporating stakeholder values into the design process.

Ensuring fairness, equity, and respect for privacy.

Addressing broader societal implications of the technology.

While privacy and human rights (option D) may be part of the values considered in VSD, its scope is broader, encompassing diverse ethical and moral issues that impact various stakeholders.

upvoted 1 times

Sourav 5 months, 3 weeks ago

Selected Answer: B

B. Ethics and morality.

Explanation: Value Sensitive Design (VSD) focuses on integrating ethical and moral values into the design process of technology and systems.

upvoted 1 times

fvo 1 year ago

B

Value-sensitive design is a design approach that accounts for moral and ethical values and should be considered when assessing the overall "value" of a design.

upvoted 1 times

dmi_air 1 year, 8 months ago

Selected Answer: B

B is correct

upvoted 1 times

SCENARIO -

Please use the following to answer the next question:

Looking back at your first two years as the Director of Personal Information Protection and Compliance for the St. Anne's Regional Medical Center in Thorn Bay,

Ontario, Canada, you see a parade of accomplishments, from developing state-of-the-art simulation based training for employees on privacy protection to establishing an interactive medical records system that is accessible by patients as well as by the medical personnel. Now, however, a question you have put off looms large: how do we manage all the data-not only records produced recently, but those still on-hand from years ago? A data flow diagram generated last year shows multiple servers, databases, and work stations, many of which hold files that have not yet been incorporated into the new records system. While most of this data is encrypted, its persistence may pose security and compliance concerns. The situation is further complicated by several long-term studies being conducted by the medical staff using patient information. Having recently reviewed the major Canadian privacy regulations, you want to make certain that the medical center is observing them.

You recall a recent visit to the Records Storage Section in the basement of the old hospital next to the modern facility, where you noticed paper records sitting in crates labeled by years, medical condition or alphabetically by patient name, while others were in undifferentiated bundles on shelves and on the floor. On the back shelves of the section sat data tapes and old hard drives that were often unlabeled but appeared to be years old. On your way out of the records storage section, you noticed a man leaving whom you did not recognize. He carried a batch of folders under his arm, apparently records he had removed from storage.

You quickly realize that you need a plan of action on the maintenance, secure storage and disposal of data.

Which cryptographic standard would be most appropriate for protecting patient credit card information in the records system at St. Anne's Regional Medical Center?

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

Suggested Answer: A

Community vote distribution



🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Symmetric Encryption

Symmetric encryption is suitable for protecting sensitive data like patient credit card information because it uses a single key for both encryption and decryption, offering strong security when the key is properly managed.

B. Tokenization is useful for protecting sensitive data by replacing it with unique tokens, but it's typically used in combination with encryption. It's not a primary cryptographic standard for encrypting data.

C. Obfuscation makes data less readable but does not provide strong security for sensitive information like credit card details. It's more about hiding data rather than securely encrypting it.

upvoted 1 times

🗨️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: C

tokenization ensures that credit card information remains protected while allowing authorized users to perform necessary tasks within the medical records system

upvoted 1 times

🗨️ 👤 **pipzz** 2 years, 6 months ago

Selected Answer: A

They are referring to data at rest here and in this case symmetric encryption can be used as per PCI DSS Guide. If the data was in motion it must be symmetric encryption.

<https://www.pcidssguide.com/encryption-key-management-essentials/>

upvoted 1 times

🗨️ **chariot** 2 years, 8 months ago

Both are cryptographic data security methods and they essentially have the same function, however they do so with differing processes and have different effects on the data they are protecting.

upvoted 1 times

🗨️ **nchzhang** 2 years, 9 months ago

Selected Answer: B

B is the answer. Tokenization is a form of encryption.

upvoted 3 times

🗨️ **Stants** 11 months, 1 week ago

The most appropriate cryptographic standard for protecting patient credit card information in the records system at St. Anne's Regional Medical Center would be B. Tokenization.

Tokenization is a process that replaces sensitive data with unique identification symbols (or "tokens") that retain all the essential information about the data without compromising its security. In the context of credit card information, tokenization can provide a high level of security because even if a token were to be intercepted or stolen, it would be useless to the thief without the original data it represents. This makes tokenization particularly suitable for protecting sensitive data like credit card numbers. It is widely used in the payment industry to reduce the scope of compliance with the Payment Card Industry Data Security Standard (PCI DSS).

upvoted 1 times

🗨️ **k4d4v4r** 3 years, 1 month ago

Found this article... <https://www.tokenex.com/blog/tokenization-vs-encryption-which-one-is-best-for-your-business>

Maybe the question is poorly written

upvoted 2 times

🗨️ **k4d4v4r** 3 years, 1 month ago

Selected Answer: A

Tokenization is a technique, not a standard.

Standards are DES, 3DES, RSA... The only "standard" being mentioned is symmetric encryption

upvoted 2 times

A privacy engineer has been asked to review an online account login page. He finds there is no limitation on the number of invalid login attempts a user can make when logging into their online account.

What would be the best recommendation to minimize the potential privacy risk from this weakness?

- A. Implement a CAPTCHA system.
- B. Develop server-side input validation checks.
- C. Enforce strong password and account credentials.
- D. Implement strong Transport Layer Security (TLS) to ensure an encrypted link.

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Implement a CAPTCHA system.

A CAPTCHA system helps to prevent automated attacks and limit the number of invalid login attempts, reducing the risk of unauthorized access and protecting user privacy.

upvoted 2 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: A

A is the right answer

upvoted 2 times

🗳️ 👤 **Stants** 11 months, 1 week ago

The best recommendation to minimize the potential privacy risk from this weakness would be A. Implement a CAPTCHA system.

A CAPTCHA system can help prevent automated attacks, such as brute force or password spraying attacks, by requiring users to prove they are human before they can proceed. This would effectively limit the number of invalid login attempts because an attacker would need to solve a CAPTCHA challenge for each attempt, which is computationally expensive and time-consuming. This makes automated attacks much less feasible. Please note that this should be used in conjunction with other security measures like account lockouts after a certain number of failed attempts, strong password policies, and encryption to provide a comprehensive security solution.

upvoted 1 times

🗳️ 👤 **chariot** 2 years, 8 months ago

B is the answer, Captcha system helps prove you are not a robot but doesnt help with authentication

upvoted 2 times

🗳️ 👤 **187san** 3 years, 1 month ago

A is the answer

upvoted 2 times

🗳️ 👤 **k4d4v4r** 3 years, 2 months ago

A is correct

upvoted 2 times

🗳️ 👤 **837vq3** 3 years, 3 months ago

why not "A"?

upvoted 1 times

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

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

Suggested Answer: C

Community vote distribution

C (88%) 13%

🗨️ **hele_meneer** 3 weeks, 3 days ago

Selected Answer: A

A and C are equally correct
upvoted 1 times

🗨️ **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. Certifying compliance with security and privacy law.

Certifying compliance with security and privacy law is typically the responsibility of compliance officers or legal professionals, not IT or software engineers.

upvoted 2 times

🗨️ **z80r** 2 years ago

Selected Answer: C

C is the right answer
upvoted 4 times

🗨️ **Sbowo** 3 years, 1 month ago

IT professional is not responsible for a privacy program but laying a good technical foundation for it (page 19 book Privacy in Technology). A is a correct answer

upvoted 1 times

🗨️ **k4d4v4r** 3 years, 1 month ago

If he can't provide feedback on privacy policies, the least he can do is to certificate compliance with privacy laws.

upvoted 1 times

🗨️ **k4d4v4r** 3 years, 1 month ago

Selected Answer: C

Can someone give an opinion?

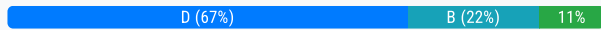
upvoted 1 times

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

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

Suggested Answer: D

Community vote distribution



🗨️ **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Descriptions of the processing activities and relevant data subjects.

The records of processing activities must include descriptions of the processing activities and relevant data subjects.

upvoted 2 times

🗨️ **z80r** 2 years ago

Selected Answer: D

I think it's D. This is not a GDPR based exam nor this question in particular mention it. So D is probably the right one.

upvoted 2 times

🗨️ **Sara_sw** 2 years, 2 months ago

Selected Answer: D

Records of processing activities must include significant information about data processing, including data categories, the group of data subjects, the processor and the data recipients. This must be completely made available to authorities upon request.

<https://gdpr-info.eu/issues/records-of-processing-activities/#:~:text=GDPR%20Records%20of%20Processing%20Activities&text=Records%20of%20processing%20activities%20must,available%20to%20authorities>

upvoted 2 times

🗨️ **pipzz** 2 years, 6 months ago

Selected Answer: C

Meant to select C in my below comment (not B)

upvoted 1 times

🗨️ **pipzz** 2 years, 6 months ago

Selected Answer: B

As per Art. 30 GDPR Records of processing activities, it's mandatory to provide name/contact details of the controller/DPO. Providing time limits is only "where possible". <https://gdpr-info.eu/art-30-gdpr/>

upvoted 2 times

🗨️ **187san** 3 years, 1 month ago

C is the answer

upvoted 1 times

After downloading and loading a mobile app, the user is presented with an account registration page requesting the user to provide certain personal details. Two statements are also displayed on the same page along with a box for the user to check to indicate their confirmation: Statement 1 reads: `Please check this box to confirm you have read and accept the terms and conditions of the end user license agreement` and includes a

- hyperlink to the terms and conditions.

⇒ Statement 2 reads: `Please check this box to confirm you have read and understood the privacy notice` and includes a hyperlink to the privacy notice.

Under the General Data Protection Regulation (GDPR), what lawful basis would you primarily expect the privacy notice to refer to?

- A. Consent.
- B. Vital interests.
- C. Legal obligation.
- D. Legitimate interests.

Suggested Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Consent.

Under the GDPR, a privacy notice should primarily refer to consent if the processing of personal data is based on obtaining explicit permission from the data subject.

upvoted 1 times

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

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

Suggested Answer: D

Reference:

<https://privacy.net/stop-cookies-tracking/>

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Manage settings in the browser to limit the use of cookies and remove them once the session completes.

This method directly addresses tracking by controlling cookie settings and ensuring they are cleared after each session.
upvoted 1 times

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

- A. Notice and consent for the downloading of data.
- B. Detection of phishing attacks against the portability interface.
- C. Re-authentication of an account, including two-factor authentication as appropriate.
- D. Validation of users with unauthenticated identifiers (e.g. IP address, physical address).

Suggested Answer: B

Community vote distribution

B (80%)

D (20%)

Ssourav 5 months, 3 weeks ago

Selected Answer: D

D. Validation of users with unauthenticated identifiers (e.g., IP address, physical address).

Data portability rights generally involve authenticated requests and proper consent mechanisms, not validation based on unauthenticated identifiers.

upvoted 1 times

Stants 11 months, 1 week ago

The option that is NOT relevant to a user exercising their data portability rights is D. Validation of users with unauthenticated identifiers (e.g. IP address, physical address).

Data portability rights, as defined by regulations like the General Data Protection Regulation (GDPR), allow individuals to obtain and reuse their personal data across different services. This involves securely transferring, copying, or moving data without hindrance to its usability.

While notice and consent for downloading data (A), detection of phishing attacks against the portability interface (B), and re-authentication of an account, including two-factor authentication as appropriate ©, are all relevant to ensuring the secure and compliant exercise of data portability rights, validating users with unauthenticated identifiers like IP or physical addresses (D) is not directly relevant

upvoted 1 times

187san 3 years, 1 month ago

B

its B

upvoted 1 times

187san 3 years, 1 month ago

Selected Answer: B

B , something related to SD

Portability, in relation to software, is a measure of how easily an application can be transferred from one computer environment to another. A computer software application is considered portable to a new environment if the effort required to adapt it to the new environment is within reasonable limits. The meaning of the abstract term 'reasonable' depends upon the nature of the application and is often difficult to express in quantifiable units.

upvoted 4 times

k4d4v4r 3 years, 1 month ago

It should be B and D in case of a multiple choice situation.

D is only plausible on a "no-login" strategy. It requires more technology to validate but it is possible to implement.

B is just bizarre. No user would ever ask for a report like that to exercise their rights.

upvoted 1 times

837vq3 3 years, 1 month ago

I am between "B" and "D". I think the question is asking for a user that is interested in "data portability" which is basically the ability to move data to somewhere else, which would NOT be useful/relevant to this user. I this "B" is NOT useful to the end-user since it should affect the company more so than the user?

upvoted 1 times

  **k4d4v4r** 3 years, 1 month ago

Can someone explain?

upvoted 1 times

In order to prevent others from identifying an individual within a data set, privacy engineers use a cryptographically-secure hashing algorithm. Use of hashes in this way illustrates the privacy tactic known as what?

- A. Isolation.
- B. Obfuscation.
- C. Perturbation.
- D. Stripping.

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Obfuscation.

Using a cryptographically-secure hashing algorithm to prevent others from identifying an individual in a dataset is a form of obfuscation, which involves disguising or masking data to protect privacy.

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 3 months ago

Obfuscation obstructs the ability to read or understand personal information. This is most commonly done with encryption or hashing but could also be done simply by using a code or little-known language.

upvoted 2 times

An organization based in California, USA is implementing a new online helpdesk solution for recording customer call information. The organization considers the capture of personal data on the online helpdesk solution to be in the interest of the company in best servicing customer calls.

Before implementation, a privacy technologist should conduct which of the following?

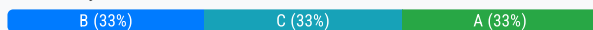
- A. A Data Protection Impact Assessment (DPIA) and consultation with the appropriate regulator to ensure legal compliance.
- B. A privacy risk and impact assessment to evaluate potential risks from the proposed processing operations.
- C. A Legitimate Interest Assessment (LIA) to ensure that the processing is proportionate and does not override the privacy, rights and freedoms of the customers.
- D. A security assessment of the help desk solution and provider to assess if the technology was developed with a security by design approach.

Suggested Answer: C

Reference:

<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>

Community vote distribution



waterdogs 4 months, 4 weeks ago

Selected Answer: B

'Legitimate Interest Assessment' is a GDPR term and GDPR requirement, not specifically required under californian law. in any case, best servicing customer calls by asking for PI doesnt sound like an ethical edge case that warrants a LIA, a DPIA or PIA of the system is more standard practice. but since consulting with a regulator is also not something i've heard any regulator do, the answer is probably B.

upvoted 1 times

moxiangnaicha 5 months, 1 week ago

Selected Answer: C

Because the question specifically mentioned this is done in the interest of the company

upvoted 1 times

waterdogs 4 months, 4 weeks ago

pretty sure 'Legitimate Interest Assessment' is a GDPR term and GDPR requirement, not specifically required under californian law. in any case, best servicing customer calls by asking for PI doesnt sound like an ethical edge case that warrants a LIA, a DPIA or PIA of the system is more standard practice. but since consulting with a regulator is also not something i've heard any regulator do, the answer is probably B.

upvoted 1 times

Ssourav 5 months, 3 weeks ago

Selected Answer: A

A. A Data Protection Impact Assessment (DPIA) and consultation with the appropriate regulator to ensure legal compliance.

A DPIA is essential for identifying and mitigating privacy risks related to the processing of personal data, especially when implementing new systems that handle customer information. It ensures compliance with data protection regulations and helps address potential privacy concerns before implementation.

upvoted 1 times

waterdogs 4 months, 4 weeks ago


consultation with the appropriate regulator? not sure that's a legitimate option for most companies and haven't heard of this being standard practice

upvoted 1 times

Ahpl 2 years, 11 months ago

why not B? Privacy and Data Protection Impact Assessments - Assessments evaluating privacy harms and issues for major activities undertaken by an organization.

upvoted 2 times

 **837vq3** 3 years, 3 months ago

<https://dataprivacymanager.net/what-is-lia-legitimate-interests-assessment-and-how-to-conduct-it/>

upvoted 1 times

Which technique is most likely to facilitate the deletion of every instance of data associated with a deleted user account from every data store held by an organization?

- A. Auditing the code which deletes user accounts.
- B. Building a standardized and documented retention program for user data deletion.
- C. Monitoring each data store for presence of data associated with the deleted user account.
- D. Training engineering teams on the importance of deleting user accounts their associated data from all data stores when requested.

Suggested Answer: C

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 2 weeks ago

Selected Answer: B

B. Building a standardized and documented retention program for user data deletion: This approach provides a structured and comprehensive framework for handling data deletion consistently across all data stores. It ensures that policies and procedures are in place for the systematic removal of data, which is crucial for achieving thorough and reliable deletion.

upvoted 2 times

🗨️ 👤 **837vq3** 3 years, 3 months ago

why not 'B'?

upvoted 1 times

🗨️ 👤 **z80r** 2 years ago

because writing a policy is formal not substantial compliance, does not assure its implementation

upvoted 2 times

🗨️ 👤 **Trepanij** 2 years, 2 months ago

Even with a good deletion program in place, how do you expect results if you dont know where is the data...

upvoted 2 times

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

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

Suggested Answer: D

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. Whether consent is durably recorded in the case of a server crash: This involves not just reviewing code but also assessing how the system handles data persistence and recovery. A code audit alone may not be able to fully test the durability of consent records in scenarios involving server crashes or other failure conditions. This requires more comprehensive testing of the system's data storage and recovery mechanisms beyond just code inspection.

upvoted 1 times

🗨️ 👤 **Stants** 11 months, 1 week ago

The option that CANNOT be effectively determined during a code audit is C. Whether consent is durably recorded in the case of a server crash.

A code audit can review the code to check for access control logic (A), data sharing practices (B), and the implementation of differential privacy (D). However, whether consent is durably recorded in the case of a server crash © is more of a system resilience and data durability issue, which typically involves infrastructure and system design rather than just the code itself. This would be better evaluated through system testing and review of infrastructure design rather than a code audit. It's also worth noting that the durability of consent recording in the event of a server crash would also depend on factors like backup and recovery strategies, which are outside the scope of a code audit.

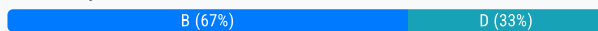
upvoted 1 times

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.

Suggested Answer: B

Community vote distribution



🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. When there is no human intervention or influence in the decision-making process: GDPR specifically addresses cases where automated decisions are made without human intervention. In such cases, individuals have the right not to be subject to solely automated decisions that have legal effects or significantly affect them, unless specific exceptions apply (e.g., explicit consent, necessary for a contract, or authorized by law with adequate safeguards).

upvoted 2 times

🗨️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: D

When the decision is necessary for entering into a contract and the individual can contest the decision: Here, the GDPR recognizes the right to object. If the decision affects contract terms, individuals can contest it.

upvoted 1 times

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:

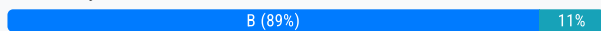
- ⇒ First and last name
- ⇒ Date of birth (DOB)
- ⇒ Mailing address
- ⇒ Email address
- ⇒ Car VIN number
- ⇒ Car model
- ⇒ License plate
- ⇒ Insurance card number
- ⇒ Photo
- ⇒ Vehicle diagnostics
- ⇒ Geolocation

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.

Suggested Answer: B

Community vote distribution



🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Allow access and sharing of geolocation data only after an accident occurs.

This approach ensures that geolocation data is only collected when necessary for the specific purpose of assessing car accident insurance claims, minimizing unnecessary data collection.

upvoted 2 times

🗳️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: A

To limit data collection to the necessary minimum while ensuring transparency and user control, the best approach would be option A: Allow users to opt-out of geolocation data collection at any time. By giving users the choice to enable or disable geolocation tracking, you respect their privacy preferences and allow them to make an informed decision about sharing their location data. This approach strikes a balance between functionality and privacy, empowering users to manage their own data usage

upvoted 1 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: B

it's B

upvoted 1 times

🗳️ 👤 **Sara_sw** 2 years, 2 months ago

Selected Answer: B

definitely not D!!

upvoted 1 times

  **187san** 3 years, 1 month ago

Selected Answer: B

B is the answer

upvoted 4 times

SCENARIO -

Please use the following to answer next question:

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

The app collects the following information:

- ⇒ First and last name
- ⇒ Date of birth (DOB)
- ⇒ Mailing address
- ⇒ Email address
- ⇒ Car VIN number
- ⇒ Car model
- ⇒ License plate
- ⇒ Insurance card number
- ⇒ Photo
- ⇒ Vehicle diagnostics
- ⇒ Geolocation

All of the following technical measures can be implemented by EnsureClaim to protect personal information that is accessible by third-parties EXCEPT?

- A. Encryption.
- B. Access Controls.
- C. De-identification.
- D. Multi-factor authentication.

Suggested Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. De-identification.

De-identification may not protect personal information if the data is still accessible by third parties and can be linked back to individuals through other means. Encryption, access controls, and multi-factor authentication directly safeguard data from unauthorized access.

upvoted 2 times

🗨️ 👤 **Sara_sw** 2 years, 2 months ago

Selected Answer: C

C is correct, since the insurance needs to know the identity of the issuer. Access control should at all cost be implemented

upvoted 2 times

🗨️ 👤 **187san** 3 years, 1 month ago

D

you can't enforce MFA on 3rd parties

upvoted 2 times

🗨️ 👤 **Scynor** 2 years, 3 months ago

Incorrect. The statement says data that 3rd parties have access to. It does not state data that they control. This means if you control the data, you control the authentication method including MFA. The reason that Access Control is the correct answer is because the question states "that they have access to". This means they already have access, ergo Access Control is not a factor at all.

upvoted 1 times

🗨️ 👤 **Stants** 1 year ago

All of the options listed - Encryption, Access Controls, De-identification, and Multi-factor authentication - are technical measures that can be implemented by EnsureClaim to protect personal information that is accessible by third-parties.

However, Option D: Multi-factor authentication is typically used to verify the identity of a user accessing the system, rather than to protect the data that is being transmitted or stored. While it adds a layer of security, it doesn't directly protect the data itself from being accessed or misused once it's been collected by the app. Therefore, in the context of the question, the answer is Option D.

upvoted 1 times

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.

Suggested Answer: D

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Client-server architecture directly aligns with the mobile app's requirement to collect data on the client side (mobile app) and process/store it on the server side. SOA is more relevant for systems requiring extensive service interactions or integrations beyond the scope of this mobile platform's primary function.

upvoted 1 times

🗨️ 👤 **Stants** 1 year ago

The most appropriate IT architecture for this mobile platform would be Option B: Client-server architecture.

In a client-server architecture, the server hosts, delivers, and manages most of the resources and services to be consumed by the client. This model would allow the mobile app (the client) to communicate with the third-party hosting provider (the server) to store and retrieve data. It would also enable EnsureClaim's customer service employees to access and review the app data from the server.

This architecture is commonly used in web applications and is well-suited to scenarios where multiple clients need to access shared data, which aligns with the needs of the EnsureClaim app. So, the answer is Option B.

upvoted 1 times

🗨️ 👤 **Sbowo** 3 years, 1 month ago

Mobile app platform usually using plug-in based architecture because it use market place of IOS and Android to be installed on mobile

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 3 months ago

Service-oriented architecture is similar to client-server architecture in that it decouples services from large-scale servers. It allows designers to replicate services across multiple machines.

upvoted 1 times

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.

Suggested Answer: C

Community vote distribution

B (100%)

🗨️ **hele_meneer** 3 weeks, 3 days ago

Selected Answer: B

Anonymizing does not imply supervising
upvoted 1 times

🗨️ **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Conduct a security and privacy review before onboarding new vendors that collect personal data from the app.

Conducting a security and privacy review before onboarding new vendors ensures that the third-party systems meet the necessary privacy and data protection standards before they handle personal data. This proactive approach helps mitigate risks related to data breaches or non-compliance.

upvoted 2 times

🗨️ **Stants** 1 year ago

The best way to supervise the third-party systems that the EnsureClaim App will share data with is Option B: Conduct a security and privacy review before onboarding new vendors that collect personal data from the app.

This approach ensures that any third-party systems have adequate security and privacy measures in place before any data is shared with them. It allows for potential issues to be identified and addressed before any personal data is put at risk.

While all the options listed are important aspects of data management and security, conducting a security and privacy review before onboarding new vendors provides a proactive approach to data protection. So, the answer is Option

upvoted 2 times

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 (WEP).
- C. Scrambling location information.
- D. Using a firewall.

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Limiting the data provided to the system.

Limiting the data provided to the GIS system helps ensure that only the necessary and relevant information is collected and stored, reducing the risk of exposure and privacy concerns.

upvoted 2 times

🗳️ 👤 **ME79** 1 year, 9 months ago

Selected Answer: A

This is a repeat of Question 68.

upvoted 1 times

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

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

Suggested Answer: D

Community vote distribution

A (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. An individual with an RFID receiver can track people or consumer products.

RFID technology can be used to track the location and movement of items or people equipped with RFID tags, posing a privacy threat if this information is accessed or used without consent.

upvoted 2 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: A

A is correct

upvoted 1 times

🗳️ 👤 **187san** 3 years, 1 month ago

A is the answer

upvoted 2 times

🗳️ 👤 **sirpuzee** 3 years, 3 months ago

The correct answer is A. RFID tags can be tracked by hidden RFID receivers and this is a real privacy threat. IAPP Privacy in technology, page 193.

upvoted 1 times

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.

Suggested Answer: D

Community vote distribution

D (100%)

🗉 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Provided notice of data sharing practices within the electronically signed rental agreement.

Incorporating the transparency principle of Privacy by Design (PbD) involves ensuring that individuals are aware of how their data will be used and shared. Providing notice of data sharing practices within the rental agreement ensures that Chuck was informed about the potential use and sharing of his data at the time of data collection, aligning with the principle of transparency.

upvoted 1 times

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).

Suggested Answer: D

Community vote distribution

D (100%)

🗉 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Transport Layer Security (TLS).

TLS is a cryptographic protocol designed to provide secure communication over a network. Using TLS ensures that Chuck's information is encrypted during transmission, protecting it from interception and unauthorized access.

upvoted 1 times

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.

Suggested Answer: A

Community vote distribution

A (100%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. By providing only the minimum necessary data to process the violation notice and masking all other information prior to transfer.

This approach limits the amount of personal information shared, reducing the risk of exposing unnecessary data and ensuring compliance with the principle of data minimization.

upvoted 1 times

SCENARIO -

Please use the following to answer the next question:

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

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

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

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

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

Suggested Answer: D

Community vote distribution

A (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

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.

This method provides a strong level of authentication by combining two pieces of information that are specific to Chuck and not easily accessible to unauthorized parties.

upvoted 2 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: A

I think it's A

upvoted 2 times

🗳️ 👤 **Ahpl** 2 years, 10 months ago

A is the better answer - last 4 ID number + unique PIN

upvoted 3 times

🗳️ 👤 **Sbowo** 3 years, 1 month ago

I think B is the answer. 2 factor authentication: driver license number and credit card information that contain name and address will be matched with data collected by Finley Motor on renting agreement

upvoted 1 times

🗳️ 👤 **187san** 3 years, 1 month ago

A

its not D,

D option is not leagal

upvoted 1 times

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

- A. Security systems can be used to enforce compliance with privacy policies.
- B. Privacy and security are independent; organizations must decide which should be 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.

Suggested Answer: C

Reference:

<https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html>

Community vote distribution

A (60%)

C (40%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

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

Security measures are critical in implementing and enforcing privacy policies by protecting personal data from unauthorized access and ensuring that data handling practices comply with privacy regulations.

Not C : While privacy restricts access to personal data based on consent and regulations, security is concerned with safeguarding data against threats and ensuring that the data is not compromised. Privacy and security are interconnected, but this statement oversimplifies their relationship.

upvoted 1 times

🗨️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: C

privacy focuses on limiting access to personal data, while security ensures the proper handling and protection of that data. Together, they create a robust framework for safeguarding information and respecting individuals' rights. ☐☐

upvoted 1 times

🗨️ 👤 **z80r** 2 years ago

Selected Answer: C

I think C is a good answer

upvoted 1 times

🗨️ 👤 **Sbowo** 3 years, 1 month ago

A not C. Security restricts access to personal information; privacy regulates how information should be used.

upvoted 3 times

🗨️ 👤 **187san** 3 years, 1 month ago

A

Its a straight forward answer

upvoted 2 times

🗨️ 👤 **k4d4v4r** 3 years, 1 month ago

Selected Answer: A

This is so weird.. but I would stick with "A"

upvoted 2 times

SCENARIO -

Please use the following to answer the next question:

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

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

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

Why is Jordan's claim that the company does not collect personal information as identified by the GDPR inaccurate?

- A. The potential customers must browse for products online.
- B. The fitness trackers capture sleep and heart rate data to monitor an individual's behavior.
- C. The website collects the customers' and users' region and country information.
- D. The customers must pair their fitness trackers to either smartphones or computers.

Suggested Answer: A

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

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

Explanation:

Under the GDPR, personal data is defined broadly to include any information that relates to an identified or identifiable individual. The data captured by the fitness trackers, such as sleep patterns and heart rate, is considered personal data because it relates to the health and behavior of individuals, and can be used to monitor and identify them. This data falls under the GDPR's definition of personal data, making Jordan's claim that the company does not collect personal information inaccurate.

upvoted 2 times

🗨️ 👤 **Sara_sw** 2 years, 2 months ago

Selected Answer: B

behaviour monitoring

upvoted 1 times

🗨️ 👤 **187san** 3 years, 1 month ago

B is the right answer

upvoted 3 times

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.

Suggested Answer: C

Community vote distribution

D (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Randomized MAC address.

Explanation:

A randomized MAC address enhances privacy by preventing tracking based on a device's fixed hardware identifier. This practice helps avoid the potential for third parties to track users through their devices over time, thereby better protecting user privacy.

upvoted 1 times

🗨️ 👤 **Sharon2000** 8 months, 1 week ago

Chat GPT says D

upvoted 1 times


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.

Suggested Answer: C

Community vote distribution

C (100%)

 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. It is a good practice to provide users with information about privacy prior to software installation.

Explanation:

Providing privacy information prior to software installation ensures users are informed about how their data will be collected, used, and protected, aligning with best practices for transparency and consent.

upvoted 1 times

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

- 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.

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Preventing data from being placed in unprotected storage.

Explanation:

Sophisticated Access Management (AM) techniques typically focus on controlling access based on factors like user role, location, and device type, but do not directly manage data storage practices or prevent data from being placed in unprotected storage. This responsibility often falls under data protection and security policies rather than access management.

upvoted 1 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: D

D is the correct one

upvoted 1 times

🗳️ 👤 **Ahpl** 2 years, 10 months ago

Pg 109 of PG - Sophisticated access management techniques can restrict access to data based on the type of data being accessed, the role of the person accessing the data, the location of the user, the time of day, or the type of device being used to access the data

upvoted 1 times

🗳️ 👤 **Ahpl** 2 years, 10 months ago

Answer is D...

upvoted 1 times

🗳️ 👤 **Sbowo** 3 years, 1 month ago

A, B, C answer is on chapter 4.2 book Privacy in Technology

upvoted 1 times

🗳️ 👤 **k4d4v4r** 3 years, 2 months ago

Selected Answer: D

Every other type is possible within IAM

upvoted 1 times

🗳️ 👤 **837vq3** 3 years, 2 months ago

I think "B" might be correct. The question is asking for what is "NOT" provided by a "sophisticated" IAM solution. Option "B" seems to be the only solution that should be standard for even the basic IAM solution.

upvoted 1 times

🗳️ 👤 **flyingrain777** 3 years, 2 months ago

Selected Answer: D

why not "D"?

upvoted 1 times

🗳️ 👤 **837vq3** 3 years, 3 months ago

why not "D"?

upvoted 1 times

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.

Suggested Answer: B

Reference:

https://www.netwrix.com/sql_server_security_best_practices.html

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. SQL injection.

Explanation:

Properly configured databases and well-written website codes can prevent SQL injection attacks by ensuring that user inputs are properly validated and sanitized before being executed in database queries. SQL injection involves inserting malicious SQL code into a query, so robust coding and database configuration are crucial for mitigating this risk.

upvoted 2 times

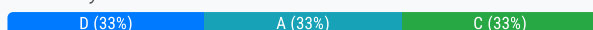
A privacy engineer reviews a newly developed on-line registration page on a company's website. The purpose of the page is to enable corporate customers to submit a returns / refund request for physical goods. The page displays the following data capture fields: company name, account reference, company address, contact name, email address, contact phone number, product name, quantity, issue description and company bank account details.

After her review, the privacy engineer recommends setting certain capture fields as `non-mandatory`. Setting which of the following fields as `non-mandatory` would be the best example of the principle of data minimization?

- A. The contact phone number field.
- B. The company address and name.
- C. The contact name and email address.
- D. The company bank account detail field.

Suggested Answer: B

Community vote distribution



🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. The company bank account detail field.

Explanation:

Setting the company bank account details field as non-mandatory exemplifies data minimization by ensuring that only necessary information is collected. Since the bank account details are not required to process a return or refund request, omitting this field reduces the amount of sensitive data collected.

upvoted 1 times

🗨️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: A

You don't necessarily have to have the contact number for a refund

upvoted 1 times

🗨️ 👤 **Stants** 11 months, 1 week ago

The best example of applying the principle of data minimization in this scenario would be:

A. The contact phone number field.

Here's why:

The contact phone number may not always be necessary for processing return/refund requests. While it can be useful for communication purposes, it may not be essential for every transaction.

By making the contact phone number field non-mandatory, the company can reduce the amount of data collected from users, aligning with the principle of data minimization.

Other fields like company name, account reference, and product details are likely essential for processing the request and may need to be mandatory to ensure the request is valid and can be efficiently handled.

Therefore, making the contact phone number field non-mandatory strikes a balance between collecting necessary information for processing requests and minimizing the collection of potentially unnecessary data.

upvoted 2 times

🗨️ 👤 **pipzz** 2 years, 6 months ago

If account reference is provided then they should not need to provide company name and address because that will be linked to account reference on the customer database.

upvoted 1 times

🗨️ 👤 **ChaChaMcGraw** 2 years, 8 months ago

Selected Answer: C

This makes no sense to me. Why is the NAME and ADDRESS of the company who wants the refund not mandatory?
upvoted 1 times

🗨️ 👤 **JPB11** 2 years, 9 months ago

This is Privacy right...i.e. individuals....A is not the right answer
upvoted 2 times

🗨️ 👤 **Ahpl** 2 years, 10 months ago

A is a better answer
upvoted 3 times

🗨️ 👤 **187san** 3 years, 1 month ago

A is the answer
upvoted 4 times

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


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

Suggested Answer: C

Community vote distribution

C (100%)



 **Ssourav** 5 months, 3 weeks ago

Selected Answer: C

C. Retention.

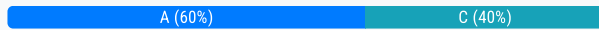
upvoted 1 times

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.

Suggested Answer: A

Community vote distribution



🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: A

A. Develop a technical privacy framework that integrates with the development lifecycle is the best method. This approach ensures that privacy principles are embedded throughout the entire development process, from initial design through implementation, rather than being considered only at specific stages or through additional tools or training.

upvoted 1 times

🗨️ 👤 **pipzz** 2 years, 6 months ago

Selected Answer: A

A framework would be the foundation on which operations and development teams can determine privacy requirements and build privacy into design at the start of all projects.

upvoted 2 times

🗨️ 👤 **Sbowo** 3 years, 1 month ago

I think it is C, both book stated Privacy review or PIA as the next step after PbD commitment

upvoted 2 times

🗨️ 👤 **k4d4v4r** 3 years, 1 month ago

PIA is only required for high risk projects and stuff like that

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 1 month ago

Selected Answer: C

Isn't "C" more appropriate?

upvoted 2 times

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.

Suggested Answer: D

Community vote distribution

D (100%)

🗳️ 👤 [Removed] 5 months ago

Selected Answer: D

Should be D

upvoted 2 times

🗳️ 👤 Ahpl 1 year, 10 months ago

A, B and C deal with transparency and choice principles. D deals with data minimization. Therefore, D is a better answer.

upvoted 2 times

🗳️ 👤 187san 2 years, 1 month ago

Selected Answer: D

D

For sure , its a straight forward question

upvoted 3 times

🗳️ 👤 837vq3 2 years, 3 months ago

I think "D" is a better choice.

upvoted 2 times

🗳️ 👤 k4d4v4r 2 years, 2 months ago

Did you already take the exam? How did it go?

upvoted 1 times

🗳️ 👤 837vq3 2 years, 2 months ago

no, not yet.

upvoted 1 times

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.

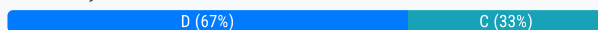
The Privacy Team is conducting a Privacy Impact Assessment (PIA) to evaluate privacy risks during development of the application. The team must assess whether the application is collecting descriptive, demographic or any other user related data from the electronic health records that are not needed for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

The Privacy Team is conducting a Privacy Impact Assessment (PIA) for the new Light Blue Health application currently in development. Which of the following best describes a risk that is likely to result in a privacy breach?

- A. Limiting access to the app to authorized personnel.
- B. Including non-transparent policies, terms and conditions in the app.
- C. Insufficiently deleting personal data after an account reaches its retention period.
- D. Not encrypting the health record when it is transferred to the Light Blue Health servers.

Suggested Answer: D

Community vote distribution



🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. Not encrypting the health record when it is transferred to the Light Blue Health servers.

Explanation: Failing to encrypt personal health records during transfer exposes them to potential interception and unauthorized access, making it a significant privacy risk and a likely cause of a privacy breach.

upvoted 2 times

🗳️ 👤 **PaigeH7** 10 months, 2 weeks ago

Selected Answer: D

encrypting health records

upvoted 1 times

🗳️ 👤 **z80r** 2 years ago

Selected Answer: D

D my friends

upvoted 1 times

🗳️ 👤 **64wlg_CBD** 2 years, 12 months ago

B. If it's a paid app it will only be accessible to paid users.

upvoted 1 times

🗳️ 👤 **Sbowo** 3 years, 1 month ago

D, the risk of privacy breach is much more higher if the data is not encrypted during transport

upvoted 3 times

🗨️ 👤 **187san** 3 years, 1 month ago

D

If you don't encrypt , PHI its breach of HIPAA security rule

upvoted 2 times

🗨️ 👤 **837vq3** 3 years, 2 months ago

Selected Answer: C

i think its C

upvoted 2 times

🗨️ 👤 **k4d4v4r** 3 years, 2 months ago

I think it's B and C.

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 2 months ago

A privacy impact assessment (PIA) is an analysis of how personal information is handled throughout the data life cycle within an organization. A PIA ensures that organizations apply legal, regulatory and policy requirements regarding privacy, assesses privacy risks, and methods of risk mitigation. A significant goal of performing a PIA is to compel an organization to think about the choices it makes for its processes and how those choices will impact privacy. Privacy technologists can utilize the findings of a PIA to determine whether privacy risk is appropriately addressed using the privacy policies and procedure

upvoted 2 times

🗨️ 👤 **837vq3** 3 years, 3 months ago

I think it should be "C"

upvoted 1 times

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.

Regarding the app, which action is an example of a decisional interference violation?

- A. The app asks income level to determine the treatment of care.
- B. The app sells aggregated data to an advertising company without prior consent.
- C. The app has a pop-up ad requesting sign-up for a pharmaceutical company newsletter.
- D. The app asks questions during account set-up to disclose family medical history that is not necessary for the treatment of the individual's symptoms.

Suggested Answer: D

Community vote distribution

A (67%)

D (33%)

🗳️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: D

D. The app asks questions during account set-up to disclose family medical history that is not necessary for the treatment of the individual's symptoms.

Explanation: Decisional interference occurs when an app requests or uses personal information that affects an individual's choices or decisions beyond what is necessary for the primary purpose of the app. Asking for family medical history not necessary for treatment affects the individual's decision-making and is an example of decisional interference.

A. The app asks income level to determine the treatment of care involves using income level to tailor recommendations or treatments. While this could raise ethical and privacy concerns, it does not directly interfere with the individual's ability to make their own decisions in a manner that would be considered decisional interference.

upvoted 1 times

🗳️ 👤 **Ahpl** 2 years, 10 months ago

A is the right answer

upvoted 1 times

🗳️ 👤 **nabomi13** 2 years, 11 months ago

Thanks to RealExamDumps for giving me pleasure by helping me out with CIPM Exam Questions. I was not sure when I downloaded this compact pdf file. Certified Information Privacy Manager (CIPM) PDF Questions proved to be very fruitful.

upvoted 1 times

🗳️ 👤 **64wlg_CBD** 2 years, 12 months ago

There is no decision to make in scenario D. A is the right answer.

upvoted 1 times

🗨️ 👤 **187san** 3 years, 1 month ago

A

No one asks for income level ,

upvoted 1 times

🗨️ 👤 **k4d4v4r** 3 years, 2 months ago

Selected Answer: A

Should be "A"

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 2 months ago

Selected Answer: A

Income should not interference with the level of care

upvoted 1 times

🗨️ 👤 **837vq3** 3 years, 3 months ago

Decisional interference is an action by an external party, such as a government or the commercial entity, that interferes with an individual's decision-making regarding their personal affairs. Inaccurate data can lead to decisional interference. Including cross-checks for accuracy when information is transferred from a manual form into an electronic form, ensuring that backup storage mechanisms allow for updating information and including individuals in the review of their information are all crucial steps privacy technologists can take to ensure information is accurate and current, thus minimizing the risk of privacy harm.

upvoted 1 times

🗨️ 👤 **k4d4v4r** 3 years, 2 months ago

So do you think it's "A"?

upvoted 1 times

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 minimize the risk of an exposure violation through the use of the app?

- A. Prevent the downloading of photos stored in the app.
- B. Dissociate the patient health data from the personal data.
- C. Exclude the collection of personal information from the health record.
- D. Create a policy to prevent combining data with external data sources.

Suggested Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **Ssourav** 5 months, 3 weeks ago

Selected Answer: B

B. Dissociate the patient health data from the personal data.

Explanation:

Dissociating patient health data from personal data minimizes the risk of exposure by ensuring that health data cannot be easily linked back to an individual without additional, separate information. This separation helps protect privacy and reduces the risk of sensitive health information being exposed or misused.

upvoted 1 times

🗨️ 👤 **ch19** 1 year, 5 months ago

D is the correct answer, as "exposure" violate means exposing an individual's data from external resources, whcih can be addressed by D

upvoted 1 times

🗨️ 👤 **frikkylanky** 1 year, 7 months ago

Who provides these answers and how do we tell what is correct. Based on studying dissociation seems like the correct answer.

upvoted 2 times

🗨️ 👤 **z80r** 2 years ago

Selected Answer: B

B for me

upvoted 1 times

🗨️ 👤 **187san** 3 years, 1 month ago

B it is