Free Questions for CIPP-US by dumpssheet

Shared by Duran on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SuperMart is a large Nevada-based business that has recently determined it sells what constitutes "covered information" under Nevada's privacy law, Senate Bill 260. Which of the following privacy compliance steps would best help SuperMart comply with the law?

Options:

A- Providing a mechanism for consumers to opt out of sales.

B- Implementing internal protocols for handling access and deletion requests.

C- Preparing a notice of financial incentive for any loyalty programs offered to its customers.

D- Reviewing its vendor contracts to ensure that the vendors are subject to service provider restrictions.

Answer:

A

Explanation:

SB 260 relates to consumer ability to opt-out of PII sales by data brokers.
https://www.leg.state.nv.us/App/NELIS/REL/81st2021/Bill/7805/Text

Question 2

Question Type: MultipleChoice

Which of the following privacy rights is NOT available under the Colorado Privacy Act?

Options:

A- The right to access sensitive data.

B- The right to correct sensitive data.

C- The right to delete sensitive data.

D- The right to limit the use of sensitive data.

Answer:

D

Explanation:

'The CPA grants Colorado Consumers new rights with respect to their personal data, including the right to access, delete, and correct their personal data as well as the right to opt out of the sale of their personal data or its use for targeted advertising or certain kinds of profiling.'

https://coag.gov/resources/colorado-privacy-act/

Even without knowing for certain the answer, one can reason that it should be D. It would be administratively difficult for businesses to adhere to varying limitation requests for each consumer... Therefore such a right would not make sense from a public policy perspective.

Question 3

Question Type: MultipleChoice

Mega Corp. is a U.S.-based business with employees in California, Virginia, and Colorado. Which of the following must Mega Corp. comply with in regard to its human resources data?

Options:

A- California Privacy Rights Act.

B- California Privacy Rights Act and Virginia Consumer Data Protection Act.

C- California Privacy Rights Act and Colorado Privacy Act.

D- California Privacy Rights Act, Virginia Consumer Data Protection Act, and Colorado Privacy Act.

Answer:

A

Question 4

Question Type: MultipleChoice

What was unique about the action that the Federal Trade Commission took against B.J.'s Wholesale Club in 2005?

Options:

A- It made third-party audits a penalty for policy violations.

B- It was based on matters of fairness rather than deception.

C- It was the first substantial U.S.-EU Safe Harbor enforcement.

D- It made user consent mandatory after any revisions of policy.

Answer:

B

Explanation:

Per the FTC Press Release in 2005, 'BJ's Wholesale Club, Inc. has agreed to settle Federal Trade Commission charges that its failure to take appropriate security measures to protect the sensitive information of thousands of its customers was an unfair practice that violated federal law.'

Question 5

Question Type: MultipleChoice

Which of the following practices is NOT a key component of a data ethics framework?

Options:

A- Automated decision-making.

B- Preferability testing.

C- Data governance.

D- Auditing.

Answer:

B

Question 6

Question Type: MultipleChoice

Once a breach has been definitively established, which task should be prioritized next?

Options:

A- Involving law enforcement and state Attorneys General.

B- Determining what was responsible for the breach and neutralizing the threat.

C- Providing notice to the affected parties so they can take precautionary measures.

D- Implementing remedial measures and evaluating how to prevent future breaches.

Answer:

B

Explanation:

IAPP Book, Section 7.4, second step. Forward looking changes are in the fourth step

Question 7

Question Type: MultipleChoice

SCENARIO -

Please use the following to answer the next question:

Jane is a U.S. citizen and a senior software engineer at California-based Jones Labs, a major software supplier to the U.S. Department of Defense and other U.S. federal agencies. Jane's manager, Patrick, is a French citizen who has been living in California for over a decade. Patrick has recently begun to suspect that Jane is an insider secretly transmitting trade secrets to foreign intelligence. Unbeknownst to Patrick, the FBI has already received a hint from anonymous whistleblower, and jointly with the National Security Agency is investigating Jane's possible implication in a sophisticated foreign espionage campaign.

Ever since the pandemic, Jane has been working from home. To complete her daily tasks she uses her corporate laptop, which after each login conspicuously provides notice that the equipment belongs to Jones Labs and may be monitored according to the enacted privacy policy and employment handbook. Jane also has a corporate mobile phone that she uses strictly for business, the terms of which are defined in her employment contract and elaborated upon in her employee handbook. Both the privacy policy and the employee handbook are revised annually by a reputable California law firm specializing in privacy law. Jane also has a personal iPhone that she uses for private purposes only.

Jones Labs has its primary data center in San Francisco, which is managed internally by Jones Labs engineers. The secondary data center, managed by Amazon AWS, is physically located in the UK for disaster recovery purposes. Jones Labs' mobile devices backup is managed by a mid-sized mobile defense company located in Denver, which physically stores the data in Canada to reduce costs. Jones Labs MS Office documents are securely stored in a Microsoft Office 365 data center based in Ireland. Manufacturing data of Jones Labs is stored in Taiwan and managed by a local supplier that has no presence in the U.S.

Before inspecting any GPS geolocation data from Jane's corporate mobile phone, Patrick should first do what?

Options:

A- Obtain prior consent from Jane pursuant to the Telephone Consumer Protection Act

B- Revise emerging workplace privacy best practices with a reputable advocacy organization.

C- Obtain a subpoena from law enforcement, or a court order, directing Jones Labs to collect the GPS geolocation data.

D- Ensure that such activity is permitted under Jane's employment contract or the company's employee privacy policy.

Answer:

D

Explanation:

'In California, it is legal to track employees during work hours. However, Californians have a constitutional right to privacy. Therefore, if you plan to track employees, make sure it's not in violation of any union agreements and that there's a documented tracking policy in place. ' https://www.workyard.com/employee-time-tracking/gps-tracking-employees-laws

Question 8

Question Type: MultipleChoice

When designing contact tracing apps in relation to COVID-19 or any other diagnosed virus, all of the following privacy measures should be considered EXCEPT?

Options:

A- Data retention.

B- Use limitations.

C- Opt-out choice.

D- User confidentiality.

Answer:

C

Explanation:

Opt-out choice is not typically a privacy measure considered in the design of contact tracing apps. Contact tracing apps are designed to help identify and notify individuals who may have been exposed to a contagious virus, such as COVID-19, in order to slow the spread of the virus. User participation in contact tracing is typically voluntary, and individuals can choose whether or not to use the app. Therefore, an opt-out choice is not directly related to the design of the app itself. Instead, it's more about user consent and participation. The other options (data retention, use limitations, and user confidentiality) are important privacy considerations in the design and operation of such apps.

Question 9

Question Type: MultipleChoice

Which of the following state laws has an entity exemption for organizations subject to the Gramm-Leach-Bliley Act (GLBA)?

Options:

A- Nevada Privacy Law.

B- California Privacy Rights Act.

C- California Consumer Privacy Act.

D- Virginia Consumer Data Protection Act

Answer:

D

Explanation:

'Nonetheless, the VCDPA will not apply to financial institutions. Specifically, the VCDPA provides that it "shall not apply to any . . . financial institutions or data subject to Title V of the federal" GLBA. In this regard, the VCDPA's GLBA exception is far broader than the CCPA's GLBA exception, which is limited only to information subject to the GLBA. That is, unlike the CCPA, the VCDPA provides not only a GLBA "information" exception, but also a GLBA "entity" exception.' https://www.mofo.com/resources/insights/210302-financial-institutions-exempt-virginia-privacy-law

Question 10

Question Type: MultipleChoice

A company based in United States receives information about its UK subsidiary's employees in connection with the centralized HR service it provides.

How can the UK company ensure an adequate level of data protection that would allow the restricted data transfer to continue?

Options:

A- By signing up to an approved code of conduct under UK GDPR to demonstrate compliance with its requirements, both for the parent and the subsidiary companies.

B- By revising the contract with the United States parent company incorporating EU SCCs, as it continues to be valid for restricted transfers under the UK regime.

C- By submitting to the ICO a new application for the UK BCRs using the UK BCR application forms, as their existing authorized EU BCRs are not recognized.

D- By allowing each employee the option to opt-out to the restricted transfer, as it is necessary to send their names in order to book the sales bonuses.

Answer:

C

Explanation:

SCCs are for transfers between third parties. BCRs are for intragroup transfers. Post Brexit, company's need to separately obtain approval with the UK ICO for their UK BCRs. 'Holders of EU Binding Corporate Rules (EU BCRs) are now required to take action to continue relying on them as an appropriate safeguard for international data.'

Question 11

Question Type: MultipleChoice

In 2011, the FTC announced a settlement with Google regarding its social networking service Google Buzz. The FTC alleged that in the process of launching the service, the company did all of the following EXCEPT?

Options:

A- Violated its own privacy policies.

B- Engaged in deceptive trade practices.

C- Failed to comply with Safe Harbor principles.

D- Failed to employ sufficient security safeguards.

Answer:

D

Explanation:

https://www.ftc.gov/news-events/news/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz-social-network

Question 12

Question Type: MultipleChoice

Which of the following statements is most accurate in regard to data breach notifications under federal and

state laws:

Options:

A- You must notify the Federal Trade Commission (FTC) in addition to affected individuals if over 500 individuals are receiving notice.

B- When providing an individual with required notice of a data breach, you must identify what personal information was actually or likely compromised.

C- When you are required to provide an individual with notice of a data breach under any state's law, you must provide the individual

with an offer for free credit monitoring.

D- The only obligations to provide data breach notification are under state law because currently there is no federal law or regulation requiring notice for the breach of personal information.

Answer:

D