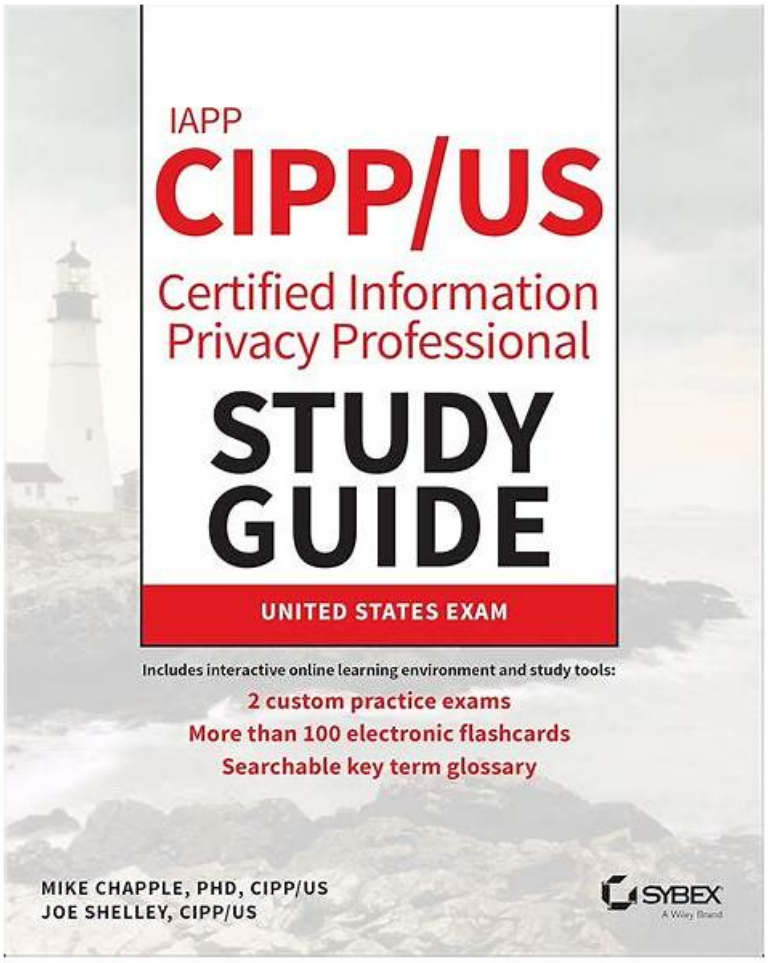
CIPP-US Prüfungs-Guide - CIPP-US German



Übrigens, Sie können die vollständige Version der ExamFragen CIPP-US Prüfungsfragen aus dem Cloud-Speicher herunterladen: https://drive.google.com/open?id=1asa0fCS4H1ptex9X2p6rHR0mCsSiTS5k

Melden Sie sich an IAPP CIPP-US Zertifizierungsprüfung an? Haben Sie vor zu vielen Prüfungsunterlagen Kopfschmerzen? Wir ExamFragen können diese Probleme auflösen und wir sind die Website, an der Sie glauben können. Wenn Sie unsere Unterlagen zur IAPP CIPP-US Prüfung benutzen, können Sie sehr leicht die IAPP CIPP-US Prüfung bestehen. Sie sollen keine Zeit an den Unterlagen verschwenden, die vielleicht keinen Sinn haben. Probieren Sie bitte den Service von ExamFragen.

Die CIPP-US-Zertifizierung wird im Bereich der Privatsphäre hoch angesehen und von Arbeitgebern auf der ganzen Welt als Zeichen des Fachwissens auf diesem Gebiet anerkannt. Personen, die die CIPP-US-Zertifizierung besitzen, sind von Arbeitgebern sehr gefragt und können häufig höhere Gehälter und angesehenere Positionen beherrschen als ihre Kollegen, die die Zertifizierung nicht besitzen.

>> CIPP-US Prüfungs-Guide <<

Die seit kurzem aktuellsten IAPP CIPP-US Prüfungsinformationen, 100% Garantie für Ihen Erfolg in der Prüfungen!

In der Gesellschaft, wo es so viele Talent gibt, stehen Sie unter dem Druck? Egal welche hohe Qualifikation Sie besitzen, kann die Qualifikation doch Ihre Fähigkeiten nicht bedeuten. Qualifikationen ist nur ein Sprungbrett und Stärke ist der Eckpfeiler, der Ihre Position verstärkt. Die IAPP CIPP-US Zertifizierungsprüfung ist eine beliebte IT-Zertifizierung. Viele Leute wollen das CIPP-US Zertifikat bekommen, so dass sie ihre Karriere machen können. Die Schulungsunterlagen zur IAPP CIPP-US Zertifizierungsprüfung von ExamFragen sind ein gutes Schulungsinstrument, das Ihnen hilft, die IAPP CIPP-US Zertifizierungsprüfung zu bestehen. Mit diesem Zertifikat können Sie international akzeptiert werden. Dann brauchen Sie sich nicht mehr zu fürchten, vom Boss gekündigt zu

werden.

Die CIPP-US-Zertifizierung wird von der International Association of Privacy Professionals (IAPP), der weltweit größten Vereinigung von Datenschutzfachleuten mit über 50.000 Mitgliedern in mehr als 100 Ländern, ausgezeichnet. Die IAPP ist bestrebt, Fachleuten, die für den Schutz personenbezogener Daten verantwortlich sind, Bildungs- und Zertifizierungsprogramme zur Verfügung zu stellen.

IAPP Certified Information Privacy Professional/United States (CIPP/US) CIPP-US Prüfungsfragen mit Lösungen (Q104-Q109):

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

- A. Virginia Consumer Data Protection Act
- B. Nevada Privacy Law.
- C. California Consumer Privacy Act.
- D. California Privacy Rights Act.

Antwort: D

Begründung:
The Virginia Consumer Data Protection Act (VCDPA) is a state law that provides comprehensive privacy rights and obligations for consumers and businesses in Virginia. The VCDPA applies to any entity that conducts business in Virginia or produces products or services that are targeted to residents of Virginia and that either: (a) controls or processes personal data of at least 100,000 consumers; or (b) controls or processes personal data of at least 25,000 consumers and derives over 50% of gross revenue from the sale of personal data. However, the VCDPA also provides several exemptions for certain types of entities and data, including an entity exemption for financial institutions or data subject to the Gramm-Leach-Bliley Act (GLBA). This means that organizations that are regulated by the GLBA are not subject to the VCDPA, regardless of the type or source of data they collect or process. The GLBA is a federal law that regulates the collection, use, and disclosure of personal financial information by financial institutions and their affiliates. The GLBA applies to any business that is significantly engaged in financial activities, such as banks, credit unions, securities firms, insurance companies, and certain fintech companies. The GLBA requires financial institutions to provide notice and choice to consumers about their privacy practices, to safeguard the security and confidentiality of consumer information, and to limit the sharing of consumer information with third parties. The GLBA also preempts state laws only to the extent that they are inconsistent with the GLBA, unless the state law provides greater protection to consumers.
The other state laws listed in the question do not have an entity exemption for organizations subject to the GLBA, but they may have partial or data exemptions for certain types of information that are regulated by the GLBA. For example, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) are state laws that provide comprehensive privacy rights and obligations for consumers and businesses in California. The CCPA and the CPRA apply to any business that collects or sells the personal information of California residents and that meets one or more of the following thresholds: (a) has annual gross revenues in excess of $25 million; (b) alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices; or derives 50% or more of its annual revenues from selling consumers' personal information. However, the CCPA and the CPRA also provide several exemptions for certain types of entities and data, including a data exemption for personal information collected, processed, sold, or disclosed pursuant to the GLBA, if it is in conflict with the GLBA. This means that information that is subject to the GLBA is exempt from the privacy requirements of the CCPA and the CPRA, but not from the data breach liability provisions. The CCPA and the CPRA do not exempt financial institutions or other entities that are regulated by the GLBA from their scope, unless they only collect or process information that is subject to the GLBA.
The Nevada Privacy Law is a state law that provides privacy rights and obligations for consumers and operators of websites or online services in Nevada. The Nevada Privacy Law applies to any person who owns or operates an Internet website or online service for commercial purposes that collects and maintains covered information from consumers who reside in Nevada and use or visit the Internet website or online service.
Covered information includes any one or more of the following items of personally identifiable information about a consumer collected by an operator through an Internet website or online service and maintained by the operator in an accessible form: (a) a first and last name; (b) a home or other physical address which includes the name of a street and the name of a city or town; an electronic mail address; (d) a telephone number; (e) a social security number; (f) an identifier that allows a specific person to be contacted either physically or online; or (g) any other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable. However, the Nevada Privacy Law also provides several exemptions for certain types of entities and data, including a data exemption for any data that is subject to the GLBA. This means that information that is regulated by the GLBA is exempt from the Nevada Privacy Law, regardless of the type or source of data. The Nevada Privacy Law does not exempt financial institutions or other entities that are subject to the GLBA from its scope, unless they only collect or process

information that is subject to the GLBA. References:
* VCDPA, Section 59.1-572 (A) (1)
* GLBA, 15 U.S.C. § 6801 et seq.
* CCPA, Section 1798.145 (e)
* CPRA, Section 1798.121
* Nevada Privacy Law, Section 603A.340 (1) (a)

105. Frage
What is the main purpose of the CAN-SPAM Act?

- A. To empower the FTC to create rules for messages containing sexually explicit content
- B. To ensure that organizations respect individual rights when using electronic advertising
- C. To authorize the states to enforce federal privacy laws for electronic marketing
- D. To diminish the use of electronic messages to send sexually explicit materials

Antwort: B

106. Frage
SCENARIO
Please use the following to answer the next question:
Larry has become increasingly dissatisfied with his telemarketing position at SunriseLynx, and particularly with his supervisor, Evan. Just last week, he overheard Evan mocking the state's Do Not Call list, as well as the people on it. "If they were really serious about not being bothered," Evan said, "They'd be on the national DNC list. That's the only one we're required to follow. At SunriseLynx, we call until they ask us not to." Bizarrely, Evan requires telemarketers to keep records of recipients who ask them to call "another time." This, to Larry, is a clear indication that they don't want to be called at all. Evan doesn't see it that way.
Larry believes that Evan's arrogance also affects the way he treats employees. The U.S.
Constitution protects American workers, and Larry believes that the rights of those at SunriseLynx are violated regularly. At first Evan seemed friendly, even connecting with employees on social media. However, following Evan's political posts, it became clear to Larry that employees with similar affiliations were the only ones offered promotions.
Further, Larry occasionally has packages containing personal-use items mailed to work. Several times, these have come to him already opened, even though this name was clearly marked. Larry thinks the opening of personal mail is common at SunriseLynx, and that Fourth Amendment rights are being trampled under Evan's leadership.
Larry has also been dismayed to overhear discussions about his coworker, Sadie. Telemarketing calls are regularly recorded for quality assurance, and although Sadie is always professional during business, her personal conversations sometimes contain sexual comments. This too is something Larry has heard Evan laughing about. When he mentioned this to a coworker, his concern was met with a shrug. It was the coworker's belief that employees agreed to be monitored when they signed on. Although personal devices are left alone, phone calls, emails and browsing histories are all subject to surveillance. In fact, Larry knows of one case in which an employee was fired after an undercover investigation by an outside firm turned up evidence of misconduct. Although the employee may have stolen from the company, Evan could have simply contacted the authorities when he first suspected something amiss.
Larry wants to take action, but is uncertain how to proceed.
In what area does Larry have a misconception about private-sector employee rights?

- A. The enforceability of local law
- B. The applicability of federal law
- C. The definition of tort law
- D. The strict nature of state law

Antwort: B

Begründung:
Larry has a misconception about the applicability of federal law to private-sector employee rights.
He believes that the U.S. Constitution protects American workers from various forms of discrimination, harassment, and invasion of privacy by their employers. However, the U.S.
Constitution only applies to government actions, not private actions, unless there is a specific federal statute that extends constitutional protections to the private sector. For example, the Civil Rights Act of 1964 prohibits discrimination on the basis of race, color, religion, sex, or national origin by private employers. The Electronic Communications Privacy Act of 1986 regulates the interception and disclosure of electronic communications by private parties. The CAN-SPAM Act of 2003 sets the rules for commercial email and gives recipients the right to opt out of receiving unwanted messages. These are examples of federal laws that apply to private-sector employees, but they do not cover all the situations that Larry faces at SunriseLynx. For instance, there is no

federal law that protects private- sector employees from political discrimination or from having their personal mail opened by their employers. Larry may have to rely on state laws or common law torts to seek redress for these violations of his rights.

107. Frage
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?

- A. Failed to employ sufficient security safeguards.
- B. Violated its own privacy policies.
- C. Engaged in deceptive trade practices.
- D. Failed to comply with Safe Harbor principles.

Antwort: A

Begründung:
The FTC alleged that Google violated its own privacy policies, engaged in deceptive trade practices, and failed to comply with Safe Harbor principles when it launched Google Buzz, a social networking service that automatically enrolled Gmail users and exposed their email contacts and other personal information without their consent or control. The FTC did not allege that Google failed to employ sufficient security safeguards, although it did require Google to implement a comprehensive privacy program and submit to regular privacy audits as part of the settlement. The other statements are incorrect because:
* A. Violated its own privacy policies: The FTC alleged that Google violated its own privacy policies by using information collected from Gmail users for a purpose that was incompatible with the purpose for which the information was collected, without obtaining their affirmative consent. Google's privacy policy stated that "When you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use."1
* B. Engaged in deceptive trade practices: The FTC alleged that Google engaged in deceptive trade practices by misrepresenting the extent to which consumers could exercise control over the collection, use, and sharing of their personal information through Google Buzz. For example, Google offered consumers the option to decline or turn off Google Buzz, but the option was ineffective and did not fully remove the consumer from the social network. Google also misled consumers about how their email contacts would be treated on Google Buzz, and failed to disclose that certain information, such as the user's frequent email contacts, would be made public by default.1
* C. Failed to comply with Safe Harbor principles: The FTC alleged that Google failed to comply with the U.S.-EU Safe Harbor Framework, which provides a method for U.S. companies to transfer personal data from the European Union to the United States in a way that meets EU data protection requirements. Google had self-certified to the Department of Commerce that it adhered to the Safe Harbor Privacy Principles, which include notice, choice, access, and enforcement. The FTC alleged that Google's conduct violated the notice and choice principles, as well as the requirement to adhere to the Safe Harbor FAQs.1 References: FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network, Google, Inc., In the Matter of, Google settles with FTC over Buzz; Privacy policies to be audited for two decades, Google Settles FTC Complaint over Google Buzz Privacy

108. Frage
SCENARIO
Please use the following to answer the next QUESTION :
A US-based startup company is selling a new gaming application. One day, the CEO of the company receives an urgent letter from a prominent EU-based retail partner. Triggered by an unresolved complaint lodged by an EU resident, the letter describes an ongoing investigation by a supervisory authority into the retailer's data handling practices.
The complainant accuses the retailer of improperly disclosing her personal data, without consent, to parties in the United States. Further, the complainant accuses the EU-based retailer of failing to respond to her withdrawal of consent and request for erasure of her personal dat a. Your organization, the US-based startup company, was never informed of this request for erasure by the EU-based retail partner. The supervisory authority investigating the complaint has threatened the suspension of data flows if the parties involved do not cooperate with the investigation. The letter closes with an urgent request: "Please act immediately by identifying all personal data received from our company." This is an important partnership. Company executives know that its biggest fans come from Western Europe; and this retailer is primarily responsible for the startup's rapid market penetration.
As the Company's data privacy leader, you are sensitive to the criticality of the relationship with the retailer.
Under the General Data Protection Regulation (GDPR), how would the U.S.-based startup company most likely be classified?

- A. As a data processor
- B. As a data manager
- C. As a data supervisor

- D. As a data controller

Antwort: A

Begründung:
Processor is the answer and correct based on the fact that the EU retailer was collecting consents and sending data internationally to US. The distractor of lack of consent and the instruction somehow implied that it now needs to be adhered to by the processor despite controller EU Retailer messing up should be mindfully sidestepped. Supervisor and Controller are synonymous with both terms used in the GDPR. Data manager is not a term used in GDPR.

109. Frage
.....