

IAPP.CIPP-US.v2025-01-27.q182

| | |
|---|--|
| 試験コード: | CIPP-US |
| 試験名称: | Certified Information Privacy Professional/United States (CIPP/US) |
| 認定資格: | IAPP |
| 無料問題数: | 182 |
| バージョン: | v2025-01-27 |
| アクセス数: | 803 |
| ページビュー数: | 1820 |
| https://www.jpnpdf.com/IAPP.CIPP-US.v2025-01-27.q182-mondaishu.html | |

最新問題: 1

より厳しい州法を優先する規定を含まない連邦法はどれですか？

- A. CAN-SPAM法
- B. 児童オンラインプライバシー保護法 (COPPA)
- C. 公正かつ正確な信用取引法 (FACTA)
- D. 電話勧誘消費者保護および詐欺防止法

Answer: D (メッセージを残す)

より厳しい州法を優先する規定を含まない連邦法は、テレマーケティング消費者保護および詐欺防止法¹である。この法律は、連邦取引委員会 (FTC) に、電話勧誘禁止登録、ロボコールの禁止、重要情報の開示など、テレマーケティング慣行に関する規則を制定および施行する権限を与えている²。しかし、この法律は、

この条項の規定の対象となる人物がテレマーケティング慣行に関する州の法律を、その州法がこの条項の規定と矛盾する場合を除き、また矛盾する場合でもその矛盾する範囲に限定して、無効にし、変更し、または影響を及ぼし、または免除すること¹。これは、州が連邦法よりも保護が劣らない限り、テレマーケティングに関する独自の法律を制定し、施行できることを意味します。対照的に、質問に挙げられている他の3つの法律には、電子通信、オンラインプライバシー、およびクレジット取引の特定の側面を規制する州の権限を制限または無効にする優先条項が含まれています^{3,4,5}。参考文献: 1: テレマーケティング消費者保護および詐欺防止法²: テレマーケティング販売規則 | 連邦取引委員会³: CAN-SPAM 法: ビジネス向けコンプライアンスガイド⁴: 児童オンラインプライバシー保護規則 (COPPA)⁵ | 連邦取引委員会⁵: 2003年公正かつ正確な信用取引法 - Wikipedia : IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第5章: 連邦取引委員会と消費者プライバシー、p.

144-145、149-150、
154-155

最新問題: 2

職場を離れた従業員に対する雇用主のプライバシー関連の責任を最もよく表しているのはどれですか？

- A. 雇用主は、差別などの会社に対する請求を裏付けるために必要なコンピュータ システムと会社のデータへの元従業員のアクセスを維持する責任があります。
- B. 雇用主は、雇用主と元従業員の両方に対するプライバシーのリスクを最小限に抑えるために、すべての機密雇用記録を永久に削除または消去する責任があります。
- C. 雇用主と従業員の関係は主に契約上のものであると考えられるため、雇用主はプライバシー関連の責任が終了したとみなすことができます。
- D. 雇用主は、正当な業務目的で保持される機密性の高い雇用記録のセキュリティとプライバシーを維持する責任があります。

Answer: D (メッセージを残す)

記録を保持する正当なビジネス上の目的は、参照、給付および年金の問い合わせ、法的手続き、法律または規制の保持要件、健康と安全の問題などに役立つ可能性があります。

最新問題: 3

組織が、高機密性として分類されたデータを低機密性として分類されたデータと同じシステムで保持する場合、最も起こり得る結果はどれですか？

- A. 組織は、ほとんどの業界固有のプライバシーおよびセキュリティ法に準拠し続けます。
- B. 組織のデータ侵害の影響は、データが分離されていた場合よりも深刻になります。
- C. 臨時従業員は、職務を遂行するために必要なデータを見つけることができます。
- D. 組織は、必要以上の情報を提出することなく、法的証拠開示要求に効率的に対応できるようになります。

Answer: B (メッセージを残す)

データ分類とは、機密性と保護のレベルを決定するために、機密性と重要性に基づいてデータを分類するプロセスです。データ分類は、組織が適切なセキュリティとコンプライアンス対策を適用して、各カテゴリが適切に保護されるようにするのに役立ちます¹。データ分類は、組織がGDPR、HIPAA、CCPAなどの特定のプライバシー法と規制の対象となるデータを特定し、データ主体の要求、データ侵害、法的証拠開示を処理する方法を決定するのにも役立ちます²。組織が、個人情報、財務情報、健康情報などの高機密に分類されたデータを、公開情報や内部情報などの低機密に分類されたデータと同じシステムで保持している場合、データ侵害が発生した場合に高機密データが漏洩するリスクが高まります。データ侵害は、法的結果、評判の低下、顧客や利害関係者からの信頼の喪失につながる可能性があります。したがって、分類に基づいてデータを分離し、各カテゴリに異なるレベルの暗号化、アクセス制御、監視を適用することをお勧めします³。このようにして、組織はデータ侵害の影響を最小限に抑え、データ資産のプライバシーとセキュリティを保護できます。参考文献:

- * データ分類が重要な理由
- * GDPR のデータ分類の説明
- * データの分類とプライバシーに関する考慮事項

最新問題: 4

カリフォルニア州在住のジョンは、年間収益 5 億ドルの大手企業でデータ侵害が発生したという通知を受け取りました。ジョンの氏名や社会保障番号など、その企業が所有していたジョンの個人情報盗まれました。ジョンはまた、その企業が彼の個人情報を保護するための適切なサイバーセキュリティ対策を講じていなかったことも知りました。

次の回答のうち、カリフォルニア州消費者プライバシー法 (CCPA) に基づいてジョンが企業に対して法的請求を追求する能力を最も正確に反映するものはどれですか？

- A. CCPA ではデータ侵害に関する権利が規定されていないため、ジョンには企業を訴える権利がありません。
- B. CCPA に基づいて訴訟を起こす権限を持つのは州の司法長官のみであるため、ジョンはデータ侵害について企業を訴えることはできません。
- C. ジョンはデータ侵害について企業を訴えることができますが、その訴えはデータ侵害の結果として実際に被った金銭的損害の回復のみを目的としています。
- D. ジョンは、データ侵害の結果として被った金銭的損害を回復するために、データ侵害について企業を訴えることができ、また、状況によっては、金銭的損害を被ったかどうかに関係なく、法定損害賠償を求めることができます。

Answer: D (メッセージを残す)

CCPA は、企業が合理的かつ適切なセキュリティを導入しなかったために、特定の機密性の高い個人情報カテゴリに影響するデータセキュリティ侵害が発生した場合、消費者に法定損害賠償を求める民事訴訟権を与えています。CCPA では、この目的での個人情報を、個人の名前と、社会保障番号、運転免許証番号、口座番号、クレジットカード番号またはデビットカード番号、医療情報、健康保険情報のいずれかとの組み合わせと定義しています。CCPA では、消費者が 1 回のインシデントにつき 100 ドルから 750 ドルの損害賠償、または実際の損害のいずれか大きい方の金額を求めることができます。また、CCPA では、訴訟を起こす前に、消費者が企業に 30 日前に書面で通知し、違反を是正する機会を与えることも義務付けています。さらに、CCPA では、訴訟を起こしてから 30 日以内に司法長官に通知し、訴訟を進める前に司法長官の承認または異議なしの回答を得ることも義務付けています。したがって、ジョンは、データ侵害の結果として被った金銭的損害を回復するために、データ侵害について企業を訴えることができ、また、CCPA の要件を満たしている限り、金銭的損害を被ったかどうかに関係なく、状況によっては法定損害賠償を求めることができます。参考資料:

- * CCPAはデータセキュリティ侵害に対する民事訴訟権を付与
- * CCPA 民事訴訟権 - データ侵害セキュリティ要件
- * データ保護違反に対する CCPA の罰金と罰則 | MatrixPoint

最新問題: 5

プライバシーに対する欧州のアプローチを支持する人の中に、プライバシー慣行の自主規制に懐疑的な人がいる主な理由は何ですか？

- A. 技術とセキュリティの向上に多額の資金を投入する必要があるかもしれない
- B. 業界はルールを作成と施行に十分厳格ではない可能性がある

C. 新規事業主は規制を理解していない可能性がある

D. プライバシーのために人権が無視される可能性がある

Answer: B (メッセージを残す)

欧州のプライバシーに対するアプローチは、プライバシーを強力な法的保護と監視を必要とする基本的人権と認識することに基づいています。EU は、一般データ保護規則 (GDPR) や ePrivacy 指令など、個人データに関わるすべての分野と活動に適用される包括的かつ拘束力のあるプライバシー法を採用しています。また、EU には、プライバシー法の遵守を監視および強制する独立したデータ保護機関 (DPA) と、プライバシー問題に関するガイダンスと意見を発行する欧州データ保護委員会 (EDPB) があります。EU は、第三国または国際機関に転送される個人データに対しても、適切なレベルのプライバシー保護を要求しています。

対照的に、米国のプライバシーに対するアプローチは、連邦法と州法、業界の行動規範、消費者教育、市場の力の組み合わせに依存するセクター別および自主規制モデルに基づいています。

U.S. には、個人データに関わるすべての分野と活動を網羅する、包括的で執行可能な連邦プライバシー法は存在しません。その代わりに、米国には、健康、金融、子供、電子通信のプライバシーなど、特定の問題や分野に対処する連邦法と州法の寄せ集めがあります。

U.S. には、連邦取引委員会 (FTC)、連邦通信委員会 (FCC)、保健福祉省 (HHS) など、プライバシー問題に関する管轄権を共有するさまざまな連邦および州機関もあります。米国はまた、プライバシーに関する自主的な行動規範、基準、ベスト プラクティスを開発し、遵守する業界による自主規制に依存しています。米国では、データ主体が同意した場合、または転送がプライバシー シールドや標準契約条項などのメカニズムによってカバーされている限り、適切なレベルのプライバシー保護を要求せずに、個人データを第三国または国際組織に転送することも許可されています。

欧州のプライバシー保護の取り組みを支持する人々の中には、プライバシー保護の自主規制に懐疑的な人々もいる。自主規制はデータ主体の権利と利益を保護するには効果的でも一貫性もなく、説明責任も十分ではないと考えているからだ。彼らは、自主規制では業界がプライバシー規則を遵守したり、プライバシーを強化する技術や慣行を採用したりするのに十分なインセンティブや制裁が与えられない可能性がある」と主張している。また、自主規制ではデータ主体の意見や期待が反映されない可能性があり、新しい技術やビジネスモデルによってもたらされる新たな複雑なプライバシーの課題に対処できないとも主張している。彼らはまた、自主規制の透明性と正当性、データ主体が権利を行使してプライバシー侵害の救済を求める能力についても疑問視している。参考文献:

* IAPP CIPP/US 学習ガイド、第 1 章: 米国のプライバシー環境の概要、9-10、16-17 ページ

* IAPPウェブサイト、CIPP/US認証

* NICCSウェブサイト、米国認定情報プライバシー専門家 (CIPP/US) トレーニング

最新問題: 6

シナリオ

次の質問に回答するには、以下を使用してください。

米国を拠点とする新興企業が新しいゲームアプリケーションを販売しています。ある日、同社の CEO は、EU を拠点とする著名な小売パートナーから緊急の手紙を受け取りました。手紙には、EU 居住者が申し立てた未解決の苦情がきっかけとなり、小売業者のデータ処理慣行に関する監督当局による調査が進行中であることが記されていました。

申立人は、小売業者が彼女の個人データを米国の当事者に同意なく不適切に開示したと非難しています。さらに申立人は、EU を拠点とする小売業者が、彼女の同意の撤回と個人データの消去要求に応じなかったと非難しています。米国を拠点とするスタートアップ企業である貴社は、EU を拠点とする小売パートナーからこの消去要求について知らされていませんでした。苦情を調査している監督当局は、関係者が調査に協力しない場合はデータフローを停止すると脅迫しています。手紙は、「当社から受け取ったすべての個人データを特定して、直ちに行動してください」という緊急の要請で締めくくられています。これは重要なパートナーシップです。会社の幹部は、最大のファンが西ヨーロッパから来ていることを知っています。そして、この小売業者は、スタートアップの急速な市場浸透の主な原因です。会社のデータプライバシーリーダーとして、あなたは小売業者との関係の重要性に敏感です。

調査のこの段階で、データ プライバシー リーダーは最初に何を確認する必要がありますか？

- A. 利用可能なデータフロー図
- B. 元の苦情の本文
- C. 同社のデータプライバシーポリシー
- D. この主題に関する現行の規制

Answer: A (メッセージを残す)

データ フロー図は、組織内または異なるエンティティ間でデータがどのように移動するかをグラフィカルに表現したものです。これにより、個人データのソース、送信先、処理方法、および各データ フローの法的根拠、保持期間、セキュリティ対策を特定できます。利用可能なデータ フロー図を確認することで、データ プライバシー リーダーは、EU を拠点とする小売パートナーからの緊急の要求に迅速かつ正確に対応できるだけでなく、データ転送プロセスにおける潜在的なリスクとコンプライアンスのギャップを評価することもできます。

データフロー図は、GDPR で高リスクの処理活動に要求されるデータ保護影響評価 (DPIA) の重要なコンポーネントでもあります。参考資料:

- * IAPP CIPP/US 知識体系、セクション II、A、2
- * [IAPP CIPP/US 学習ガイド、第 2 章、セクション 2.3]
- * [GDPR、第35条]

最新問題: 7

この通知をお読みください:

当社のウェブサイトでは Cookie を使用しています。Cookie を使用すると、サイトにアクセスするために使用しているコンピューターまたはデバイスを識別できますが、個人を特定するものではありません。Web ブラウザで Cookie を拒否するように設定する方法については、[ここをクリックしてください](#)。

通知ではどのような種類の法的選択肢が提供されないのでしょうか？

- A. 暗黙の同意
- B. オプトアウト
- C. オプトイン
- D. 必須

Answer: B ([メッセージを残す](#))

最新問題: 8

シナリオ

次の質問に答えるには、以下を使用してください。

シェリルは、Fitness Coach, Inc. の唯一の所有者です。同社は、クラス、個人指導、大規模な屋内ジムへのアクセスを通じて、個人のフィットネス目標の実現を支援する中規模企業です。彼女は 10 年間この会社を経営しており、常に最高レベルのサービスを維持しながら顧客のプライバシーを保護することに配慮してきました。彼女は、顧客と長期にわたる関係を築いてきたことを誇りに思っています。

シェリルとスタッフはプライバシー保護を最優先にしようと努めてきましたが、会社には正式なプライバシー ポリシーがありませんでした。そこでシェリルはプライバシーの専門家であるジャニスを雇い、ポリシーの作成を手伝ってもらいました。

最初の評価の後、ジャニスは新しいポリシーの最初のものを作成しました。シェリルは草案を読み、このポリシーが会社全体にもたらす多くの変更を懸念しました。たとえば、草案では、パーソナルトレーナーとのセッションなどのサービスに対して顧客の個人情報を支払った後、1年間のみ保持できると規定されています。また、顧客の書面による同意なしに顧客情報を第三者と共有しないことも約束しています。これらの規則の文言はシェリルを心配させます。なぜなら、保存された個人情報は、顧客が長い間訪問していなくても、会社が顧客にサービスを提供するのに役立つことが多いからです。さらに、契約ベースでクラスを教えるエアロビクスのインストラクターなど、重要なサービスを提供するサードパーティもいます。顧客ファイルにアクセスし、生徒のフィットネスレベルを理解することは、インストラクターがクラスを編成するのに役立ちます。

ジャニスはシェリルの懸念を理解し、すでにいくつかの修正案を練っていました。顧客データは保持できるが、機密性のレベルに応じて分類する必要があることを指摘して、シェリルを安心させようとしていました。しかし、シェリルは懐疑的でした。データを分類し、タイプごとに異なる取り扱いをすると、会社の日常業務に不必要な困難が生じるように思われました。シェリルは、必要に応じてすべての従業員がアクセスできる、1つのシンプルなデータ ストレージおよびアクセス システムを望んでいます。

プライバシー ポリシーはまだ草案に過ぎませんでした。彼女は社内に変更が必要になるだろうと感じ始めていました。彼女はジャニスに、数か月かけて 1 部門ずつ新しいポリシーを徐々に導入する方が安心できるだろうと伝えました。また、新しいポリシーの適用可能な部分を各部門にリストしたドキュメントを作成するという階層化アプローチにも興味がありました。

顧客データの分類に関するジャニスの提案にシェリルが従うべき最も良い理由は何ですか？

- A. 従業員の組織化に役立ちます
- B. 連邦政府の義務を果たすのに役立つ
- C. 顧客の個人情報 (PI) のセキュリティを強化します
- D. 企業が個人情報 (PI) を過剰に収集することを防ぎます。

Answer: ([解答を表示する](#))

説明/参照: https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/dcps/

最新問題: 9

グローバル プライバシー エンフォースメント ネットワークの主な目的は何ですか?

- A. プライバシー当局間の普遍的な協力を促進する
- B. 国際的にプライバシー侵害の申し立てを調査する
- C. 世界中のプライバシー消費者団体の利益を保護するため
- D. プライバシー法の管轄権をめぐる国家間の紛争を仲裁する

Answer: A ([メッセージを残す](#))

グローバル プライバシー エンフォースメント ネットワーク (GPEN) は、プライバシー エンフォースメント機関 (PEA) がプライバシーのエンフォースメントと協力の実際的な側面に関する知識、経験、ベスト プラクティスを共有するためのネットワークです。GPEN は、OECD のプライバシー保護法の執行における国境を越えた協力に関する勧告に応じて作成されました。この勧告では、加盟国に PEA の非公式ネットワークの設立を促進するよう求めています。GPEN の主な目的は、特に複数の管轄区域または地域が関係する場合に、PEA 間の国境を越えた協力と調整を促進することです。また、GPEN は、PEA 間の情報共有を強化し、意識と教育を促進し、能力開発を支援することも目的としています。参考文献:

- * ホーム (パブリック) | グローバルプライバシーエンフォースメントネットワーク
- * グローバルプライバシー執行ネットワーク - 国際プライバシー専門家協会
- * 国際パートナーシップ - カナダプライバシーコミッショナー事務所
- * 専門ネットワーク - グローバルプライバシーアセンブリ
- * グローバルプライバシー執行ネットワーク (GPEN) の行動計画
- * [IAPP CIPP/US 認定情報プライバシー専門家学習ガイド]、第 6 章、213 ページ。

最新問題: 10

シナリオ

次の質問に回答するには、以下を使用してください。

ある晩、マットは息子の寝室に行き、息子がベッドに寝そべてノートパソコンを打っているのを見つけた。

「ネットワークを構築中ですか？」とマットは期待を込めて尋ねた。

「いいえ」少年は言った。「アンケートに答えているところです。」

マットは息子の肩越しに自分のコンピューターの画面を見た。「どんな調査？」私の意見についての質問だよ。」

「ちょっと見てみよう」とマットは言い、息子がすでに答えた質問のリストを読み始めた。政府と市民権についての意見を聞いているんだ。ちょっと変だな。君はまだ10歳なのに。」マットは、どうしてこのアンケートのウェブラックが息子のメールの受信箱に入ってしまったのか不思議に思った。このメッセージは息子に間違っただけで送られたのかもしれないと思い、開いて読んでみた。このメッセージは、リーダーシップ プロジェクトという団体から送られてきたもので、内容と画像から子供向けであることがわかった。マットが読み進めると、アンケートに答えた子供は自動的に、有名なリーダーに関するシリーズの最初の本が当たるコンテストに登録されることがわかった。

マットにとって、これは明らかに子供たちに商品やサービスを売り込むためのマーケティング戦略に思えました。彼は息子に、アンケートに答えるために自分自身の情報を提供するよう求められたかどうか尋ねました。息子は、名前、住所、電話番号、生年月日を尋ねられ、好きなゲームやおもちゃについての質問に答えるよう求められたと答えました。

マットは心配していました。マーケティング担当者が息子からこのような方法で情報を収集することが合法かどうか疑問に思いました。その後、息子の受信箱に子供向けの商品を宣伝するマーケティング担当者からの他のいくつかの商業メールが届いていることに気づき、この事件を適切な当局に報告する時だと判断しました。

マットはどのようにしてマーケティング担当者の活動を報告する決断をしたのでしょうか？

- A. マーケティング担当者はマットに情報を提供するための適切な努力を怠った
- B. マーケティング担当者は、賞品となる本が子供向けに適切であるという証拠を提示しなかった。
- C. マーケターはマットの許可なく息子の情報を配布したようだ
- D. マーケターは、自分自身の身元を明らかにせず、メッセージの目的を示さなかった

Answer: C (メッセージを残す)

マットがマーケターの活動を報告しようとしたのは、マーケターが児童オンラインプライバシー保護法 (COPPA) に違反しているのではないかと疑いがあったためです。COPPA は、13 歳未満の児童からの個人情報のオンライン収集、使用、開示を規制する連邦法です。COPPA によると、児童を対象とした、または児童から故意に個人情報を収集する Web サイトやオンライン サービスの運営者は、次の義務を負います。

- * 子どもから個人情報を収集、使用、開示する前に、情報の取り扱いについて保護者に通知し、検証可能な保護者の同意を得ます¹²。
- * 保護者に対して、運営者が子供の情報を収集し、内部で使用することに同意するが、運営者がその情報を第三者に開示することを禁止する選択肢を与える (ただし、開示がサイトまたはサービスに不可欠な場合は、保護者にその旨を明確に伝える必要がある)¹²。
- * 保護者が子供の個人情報にアクセスして確認したり、削除したりできるようにし、子供の個人情報のさらなる使用やオンラインでの収集を防ぐ機会を保護者に提供します¹²。
- * 子供から収集した情報の機密性、セキュリティ、完全性を維持し、その情報を機密性とセキュリティを維持できる当事者にのみ公開するための合理的な措置を講じるなどします¹²。
- * オンラインで子供から収集した個人情報は、収集目的を達成するために必要な期間のみ保持し、不正アクセスや不正使用を防ぐために合理的な手段で削除します¹²。

* 子供から収集した個人情報の機密性、セキュリティ、完全性を保護するための合理的な手順を確立し、維持します¹²。

マットの場合、彼はマーケティング担当者からアンケートやコンテストに関する通知を受け取っておらず、息子の個人情報の収集や開示に同意していませんでした。また、息子の情報にアクセスしたり管理したりすることもできず、さらなる使用や収集を防ぐこともできませんでした。さらに、息子の受信箱に入っている商用メールから、息子の情報が他のマーケティング担当者と共有されている可能性があることに気付きました。これらの行為は、マーケティング担当者が COPPA の要件を遵守しておらず、息子の情報を権限のない、または不適切な相手にさらした可能性があることを示唆しています。そのため、マットは、COPPA を施行し、違反に対して民事罰を課すことができる連邦取引委員会 (FTC) などの適切な当局にマーケティング担当者の活動を報告することにしました¹³。参考文献: 1:

児童オンラインプライバシー保護法 | 連邦取引委員会、1. 2: 16 CFR Part 312 - 児童オンラインプライバシー保護規則、3. 3: 児童オンラインプライバシー保護法 - Wikipedia、2.

最新問題: 11

職場を離れた従業員に対する雇用主のプライバシー関連の責任を最もよく表しているのはどれですか？

- A. 雇用主と従業員の関係は主に契約に基づくものと考えられるため、雇用主はプライバシー関連の責任は終了したとみなすことができます。
- B. 雇用主は、差別などの会社に対する請求を裏付けるために必要なコンピュータ システムと会社のデータへの元従業員のアクセスを維持する責任があります。
- C. 雇用主は、正当な業務目的で保持される機密性の高い雇用記録のセキュリティとプライバシーを維持する責任があります。
- D. 雇用主は、雇用主と元従業員の両方に対するプライバシーのリスクを最小限に抑えるために、すべての機密雇用記録を永久に削除または消去する責任があります。

Answer: ([解答を表示する](#))

最新問題: 12

生徒が高校を卒業し、公立の高等教育機関に通っています。どのような条件であれば、学校は生徒の両親の同意なしに教育記録を合法的に開示できますか？

- A. 学生がまだ18歳になっていない場合
- B. 学生が停学処分を受ける恐れがある場合
- C. 学生が税務上の扶養家族である場合
- D. 学生が他の教育機関への転校を申請している場合

Answer: C ([メッセージを残す](#))

説明/参照: <https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpafaq.pdf>

最新問題: 13

シナリオ

次の質問に回答するには、以下を使用してください。

デクランさんはウッドランド病院の放射線科で看護助手として働き始めたばかりです。また、正看護師になるためのプログラムも始めました。

このキャリアに進む前、デクランは医療保険の携行性と責任に関する法律 (HIPAA) について漠然と知っていました。彼は現在、患者の保護対象医療情報 (PHI) のセキュリティを確保するために尽力する必要があることを認識しており、プライバシーの問題について慎重に考えています。

初日の朝、デクランは、新しく雇われた受付係が各患者に HIPAA プライバシー通知を渡していることに気づきました。彼は、再診患者にこれらのプライバシー通知を渡す必要があるかどうか、また、放射線科部門が 1 回限りの配布システムによって紙の無駄を減らせないかと考えました。

彼はまた、病院が請求会社を利用していることにも興味を持っていました。請求会社が患者の治療に関する詳細を知っている場合、病院は患者のプライバシーを保護するためにできる限りのことをしているのだろうかと疑問を呈しました。

初日にデクランは、病院の大きな放射線科のすべてのエリアに精通しました。途中で残された機器を整理していたとき、彼は 2 人の病院管理者の会話を耳にしました。彼は、暗号化されていない患者情報を含むポータブルハードドライブが紛失したと聞いて驚きました。管理者は、病院が責任を回避できることに安堵しました。デクランは驚き、何が起こったのか病院が適切に報告する計画があるかどうか疑問に思いました。

デクランはこの問題について懸念を抱いていたものの、電子医療記録 (EHR) を患者の日常的なケアに統合しようとする病院の取り組みに驚きました。全国のすべての医療施設で EHR にアクセスできれば、ケアをさらに効率化できる可能性があると考えました。

デクランは患者と多くの良い関係を築いた。初日の終わりに、彼はジョンという患者と話をした。彼の父親は変性性筋疾患と診断されたばかりだった。ジョンは血液検査を受けるところだったが、血液検査で病気の遺伝的素因が明らかになり、保険適用を受けられなくなるのではないかと心配していた。デクランはジョンに、そんなことはあり得ないと思うと伝えたが、患者は理由を説明する前に車椅子で運び去られてしまった。ジョンはこの件について同僚に尋ねるつもりだ。

デクランは、1 か月後に、自分の選んだ健康に関するトピックの授業でレポートを提出しなければなりません。それまでに、デクランは、事例として使える患者とのやり取りをたくさん経験しているでしょう。遺伝子検査についてもっと慎重に考えるきっかけを与えてくれたジョンに、デクランは名前を挙げて感謝の意を表すでしょう。

デクランの一日は多くの質問で終わりましたが、彼は新しい役職に満足していました。

このシナリオに基づいて、デクランの上司が病院の請求会社の使用に関する質問に最もよく答える方法は何でしょうか？

- A. デクランに病院が公表しているプライバシーポリシーを確認するよう提案することで
- B. デクランに、第三者が個人医療情報 (PHI) を閲覧できないように保証することで
- C. 最低限のセキュリティ基準の遵守を確実にするために契約が締結されていることを指摘することで

D. 請求システムが病院の電子医療記録 (EHR) システムにどのように統合されているかを説明する

Answer: C (メッセージを残す)

HIPAA では、病院などの対象事業体は、保護対象医療情報 (PHI) にアクセス、使用、または開示するビジネス アソシエート (請求会社など) と契約を結ぶことが義務付けられています。ビジネス アソシエート契約 (BAA) と呼ばれるこれらの契約では、ビジネス アソシエートによる PHI の使用と開示の許可と義務、およびビジネス アソシエートが PHI のプライバシーとセキュリティを保護するために従わなければならない保護手段、報告、および終了手順を指定する必要があります。これらの契約を締結することで、病院は請求会社が HIPAA に準拠し、法律で義務付けられている最低限のセキュリティ基準を遵守していることを保証できます。参考資料:

* 医療費請求に関する HIPAA 規則 - コンプライアンス グループ

* 請求会社向け HIPAA コンプライアンス: 簡単ガイド - iFax

最新問題: 14

シナリオ

次の質問に回答するには、以下を使用してください。

あなたは、米国州 A の大都市にある主要病院 HealthCo の最高プライバシー責任者です。HealthCo は HIPAA の対象事業体であり、100,000 人以上の患者に医療サービスを提供しています。サードパーティのクラウド コンピューティング サービス プロバイダーである CloudHealth は、HealthCo に代わってこれらの個人の電子保護医療情報 (ePHI) を保存および管理しています。CloudHealth はデータを州 B に保存します。HealthCo と CloudHealth とのビジネス アソシエート契約 (BAA) の一環として、HealthCo はデータを適切に保護するために、業界標準の暗号化手法を含むセキュリティ対策を CloudHealth に実装することを要求しています。

しかし、HealthCo は契約締結前に CloudHealth に対するデューデリジェンスを実施しておらず、CloudHealth のセキュリティ対策の監査も実施していません。

CloudHealth の従業員が最近フィッシング攻撃の被害者になりました。従業員が不審なメールのリンクをうっかりクリックしたため、HealthCo の患者 10,000 人以上の PHI が侵害され、その後、その情報がオンラインで公開されました。HealthCo のサイバーセキュリティチームは、犯人が他の病院に対して同様の攻撃を仕掛けた既知のハッカーであることをすぐに特定しました。この攻撃では、著名人や政治家などの公人の PHI が漏洩しました。

調査の過程で、HealthCo は、CloudHealth が契約条件に従って PHI を暗号化していなかったことを発見しました。さらに、CloudHealth は従業員にプライバシーやセキュリティに関するトレーニングを提供していませんでした。法執行機関は、HealthCo に対し、侵害に関する調査報告書と影響を受けた個人の PHI のコピーを提供するよう要求しました。

侵害の影響を受けた患者は、HealthCo 社が個人の ePHI を適切に保護しなかったため、漏洩したデータによって患者が多大な損害を被ったと主張して同社を訴えました。患者の弁護士は、侵害で漏洩した ePHI に関する証拠開示請求を提出しました。

HIPAA セキュリティ ルールで要求される安全対策のうち、HealthCo の行動によって問題にならないのは次のどれですか。

- A. 管理上の安全策
- B. 技術的安全対策
- C. 物理的な安全対策
- D. セキュリティ保護

Answer: D (メッセージを残す)

HIPAA セキュリティ ルールでは、対象となる事業体とそのビジネス アソシエイトが、電子的に保護された医療情報 (ePHI) の機密性、整合性、可用性を保護するために、管理、物理、技術の 3 種類の保護手段を実装することを義務付けています¹。セキュリティ保護手段は、保護手段の個別のカテゴリではなく、3 種類すべてを網羅する一般的な用語です。したがって、これは質問に対する正しい回答ではありません。

* 管理上の保護手段とは、従業員の実行と、ePHI を保護するために導入されるセキュリティ対策を管理するポリシーと手順です。これには、リスク分析と管理、トレーニング、緊急時対応計画、インシデント対応、評価が含まれます¹²。

* 物理的な保護手段とは、電子 PHI への不正アクセスを防ぐためのロック、ドア、カメラ、その他の物理的な手段です。これには、ワークステーションとデバイスのセキュリティ、ロックとキー、メディアの廃棄が含まれます¹²。

* 技術的保護手段とは、ePHI を不正アクセス、改ざん、破壊から保護するソフトウェアおよびハードウェア ツールです。これには、アクセス制御、暗号化、監査制御、整合性制御、および伝送セキュリティが含まれます¹²。

このシナリオでは、HealthCo の行動が 3 種類の安全策すべてに違反している可能性があります。例:

* HealthCo は、契約締結前に CloudHealth に対するデューデリジェンスを実施しておらず、CloudHealth のセキュリティ対策の監査も実施していません。これは、リスク分析および管理に関する管理上の安全策の違反となる可能性があります¹²。

* HealthCo は、CloudHealth が契約条件に従って PHI を暗号化していないことを発見しました。これは暗号化の技術的保護手段の違反となる可能性があります¹²。

* HealthCo は、侵害に関する調査報告書と影響を受けた個人の PHI のコピーを法執行機関に提供します。HealthCo が移転後にメディアが適切に消去または破棄されたことを確認しなかった場合、これはメディアの廃棄に関する物理的保護措置の違反となる可能性があります¹²。

参考資料: 1: HIPAA セキュリティ ルールの概要、HHS.gov。2: HIPAA セキュリティ ルールとは何ですか?

安全対策... - Secureframe、Secureframe.com。

最新問題: 15

サラさんはカリフォルニア州サンフランシスコに住んでいます。迷惑な商業メールが急増していることから、5,000 万人以上のユーザーを抱える大手ソーシャル メディア プラット

フォームがサラさんの個人情報を大量に収集しているのではないかと考えています。このプラットフォームを運営する会社はニューヨークとフランスに拠点を置いています。なぜサラはソーシャルメディアプラットフォームに対して、彼女について収集された個人情報を削除するよう要求する権利があるのでしょうか？

- A. ヨーロッパに拠点を置く企業は、データ主体の削除要求への対応を含め、世界的に一般データ保護規則に準拠する必要があります。
- B. FTC 法第 5 条に基づき、連邦取引委員会は、個人の個人情報の削除要求を拒否することは不公正な行為に当たると判断しました。
- C. カリフォルニア州消費者プライバシー法により、サラは自分の個人情報の削除を要求する権利を有します。
- D. ニューヨーク州の「ハッキングを阻止し、電子データセキュリティを強化する」(SHIELD) 法では、ニューヨーク州の管轄下にある企業は、要求に応じて顧客の個人情報を削除することが義務付けられています。

Answer: C (メッセージを残す)

説明/参照: <https://www.varonis.com/blog/ccpa-vs-gdpr/>

最新問題: 16

違反が確実に確認されたら、次にどのタスクを優先すべきでしょうか？

- A. 法執行機関と州司法長官が関与しています。
- B. 侵害の原因を特定し、脅威を無力化します。
- C. 影響を受ける当事者に通知して予防措置を講じられるようにします。
- D. 是正措置を実施し、将来の違反を防ぐ方法を評価します。

Answer: (解答を表示する)

IAPP CIPP/US 学習ガイドによると、違反が確認された後の最優先事項は、法律または契約で義務付けられているように、影響を受けた個人、規制当局、およびその他の利害関係者に通知することです。これは、個人情報の盗難、詐欺、評判の失墜などの潜在的な危害から身を守るための措置を講じることができるようにするためです。タイムリーで正確な通知を提供することは、法的責任を軽減し、顧客の信頼を維持し、適用される法律や規制に準拠するのに役立ちます。その他のタスクも重要ですが、違反が確認された後の当面の優先事項ではありません。参考文献: IAPP CIPP/US 学習ガイド、第 6 章、セクション 6.4.2、211 ページ。

有効な CIPP-US 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集！ GoShiken.com が最新の CIPP-US 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (22830%OFF問題集溶と正解付きで 30%w 特別割引コード:

Freepdfdumps)

最新問題: 17

保健福祉省 (HHS) 内のどの組織が医療保険の携行性と責任に関する法律 (HIPAA) の「プライバシー規則」を主に施行していますか？

- A. 公民権局。
- B. 社会福祉局。
- C. 監察総監室。
- D. 公衆衛生安全局。

Answer: ([解答を表示する](#))

HHS 内の公民権局 (OCR) は、HIPAA プライバシー ルールの主な執行機関です。このルールは、対象となる事業体とビジネス アソシエイトによる個人識別可能な健康情報の保護に関する国家基準を確立しています。OCR は苦情を調査し、コンプライアンス レビューを実施し、プライバシー ルールの遵守を確保するための技術支援とガイダンスを提供します。OCR は、プライバシー ルール違反に対して民事罰金を課すこともできます。罰金は 1 回の違反につき 100 ドルから 50,000 ドルの範囲で、同じ違反に対して年間最大 150 万ドルです。参考資料: HIPAA の施行、IAPP CIPP/US 学習ガイド、第 3 章、セクション 3.1.1

最新問題: 18

「民事訴訟権」を最もよく表しているのは次のどれですか？

- A. 個人が自分の情報へのアクセスを要求する権利。
- B. 法律違反によって被害を受けた個人が、その違反に対して訴訟を起こす権利。
- C. 個人が自分の情報を秘密に保つ権利。
- D. データ処理によって被害を受けた個人が自分の情報を削除する権利。

Answer: ([解答を表示する](#))

最新問題: 19

データ侵害通知法を制定しているほとんどの州では、影響を受けた個人への通知は、「不当な遅延なく可能な限り迅速に」。対照的に、影響を受ける個人への通知に明確な制限を現在課している州は次のどれですか。

- A. メイン
- B. フロリダ
- C. ニューヨーク
- D. カリフォルニア

Answer: ([解答を表示する](#))

定義済みツールの Web 検索結果によると、フロリダ州は、データ侵害が発生した場合に影響を受ける個人への通知に現在明確な制限を設けている 4 つの選択肢の中で唯一の州です。フロリダ州の法律では、法執行機関または侵害の範囲を特定してシステムの整合性を回復するための措置によって遅延されない限り、侵害の確定または侵害が発生したと信じる理由から 30 日以内に通知を提供することが義務付けられています¹。他の州では、通知の期限について、「できるだけ早く」(メイン州)、可能な限り迅速に、不当な遅延なく」(ニューヨーク州)、

法執行機関の正当なニーズに合わせて、可能な限り迅速に、不当な遅延なく」(カリフォルニア州) など、より柔軟または曖昧な条件が使用されています²。参考文献:

* セキュリティ侵害通知チャート | Perkins Coie

* 州データ侵害通知チャート - 国際データ侵害協会

最新問題: 20

州の違反通知法では、個人情報の定義に通常含まれないものは何ですか?

- A. 州識別番号
- B. 名と姓
- C. 社会保障番号
- D. 医療情報

Answer: ([解答を表示する](#))

州の侵害通知法では、個人情報は通常、個人のファーストネームまたはファーストネームのイニシャルと姓に、社会保障番号、州識別番号、口座番号、医療情報などの1つ以上の他のデータ要素を加えたものと定義されています。ただし、ファーストネームと姓のみは、個人を特定したり、セキュリティやプライバシーを侵害したりする可能性のある他のデータ要素と組み合わせない限り、通常は個人情報とは見なされません。したがって、オプション B は、州の侵害通知法の下での個人情報の定義に通常は含まれていないため、正解です。参考文献:
<https://www.ncsl.org/technology-and-communication/security-breach-notification-laws>[https://](https://www.ncsl.org/technology-and-communication/security-breach-notification-laws)

最新問題: 21

製薬会社の CFO がフィッシングメールに騙され、会社の従業員の人事ファイルの多くをオンラインの悪者に公開してしまいました。ファイルには、従業員の連絡先情報、求人応募、業績評価、懲戒記録、職務内容などが含まれています。

次の州法のうち、影響を受けた従業員が雇用主に対して取れる最善の手段はどれでしょうか?

- A. 州の社会保障番号機密保持法。
- B. 州の人事記録審査法。
- C. 州のデータ破棄法。
- D. 州の UDAP 法。

Answer: ([解答を表示する](#))

州の人事記録審査法は、通常、従業員の人事記録へのアクセス、維持、保護を規定していません。従業員が自分の人事記録にアクセスする特定の権利を確立し、データセキュリティや従業員情報の漏洩に関する規定も含まれる場合があります。開示された情報には従業員の連絡先情報、求人応募、業績評価、その他の人事関連データが含まれるため、影響を受ける従業員は、この法に基づいて、個人情報や機密情報の漏洩に関連する救済策や保護を求める可能性があります。

最新問題: 22

シナリオ -

次の質問に答えるには、以下を使用してください。

ジェーンは米国市民で、カリフォルニアに拠点を置くジョーンズ ラボの上級ソフトウェアエンジニアです。ジョーンズ ラボは米国国防総省やその他の米国連邦政府機関にソフトウェアを供給する大手企業です。ジェーンのマネージャーであるパトリックはフランス市民で、カリフォルニアに 10 年以上住んでいます。パトリックは最近、ジェーンが外国の諜報機関に秘密裏に企業秘密を漏らしている内部関係者ではないかと疑い始めました。パトリックは知りませんでした。FBI はすでに匿名の内部告発者からヒントを得ており、国家安全保障局と共同でジェーンが高度な外国スパイ活動に関与している可能性を調査しています。

パンデミック以来、ジェーンは在宅勤務をしています。彼女は日々の業務をこなすために会社のノートパソコンを使用していますが、ログインするたびに、機器はジョーンズ ラボの所有物であり、制定されたプライバシー ポリシーと雇用ハンドブックに従って監視される可能性があることが目立つように表示されます。ジェーンは会社の携帯電話も所有しており、これは仕事にのみ使用しています。その条件は雇用契約で定義され、従業員ハンドブックで詳しく説明されています。プライバシー ポリシーと従業員ハンドブックは、プライバシー法を専門とするカリフォルニアの評判の高い法律事務所によって毎年改訂されています。ジェーンは私用 iPhone も所有しており、私的な目的にのみ使用しています。

Jones Labs はサンフランシスコに主要なデータセンターを構えており、Jones Labs のエンジニアによって社内管理されています。

Amazon AWS が管理するセカンダリ データ センターは、災害復旧を目的として物理的には英国にあります。Jones Labs のモバイル デバイスのバックアップは、デンバーにある中規模のモバイル ディフェンス会社によって管理されており、コスト削減のため物理的にはカナダにデータを保管しています。Jones Labs の MS Office ドキュメントは、アイルランドにある Microsoft Office 365 データ センターに安全に保管されています。Jones Labs の製造データは台湾に保管されており、米国には拠点のない現地のサプライヤーによって管理されています。

ジェーンの会社の携帯電話から GPS 位置情報データを調べる前に、パトリックはまず何をすべきでしょうか？

- A. 電話消費者保護法に従ってジェーンから事前の同意を得る
- B. 信頼できる擁護団体と協力して、職場のプライバシーに関する新たなベストプラクティスを改訂します。
- C. 法執行機関からの召喚状、または裁判所命令を取得し、Jones Labs に GPS 地理位置データの収集を指示します。
- D. そのような活動がジェーンの雇用契約または会社の従業員プライバシー ポリシーで許可されていることを確認します。

Answer: [\(解答を表示する\)](#)

パトリックはまず、ジェーンの雇用契約または会社の従業員プライバシー ポリシーで、ジェーンの会社の携帯電話から GPS 位置情報データを調べることに許可されていることを確認する必要があります。これは、ジェーンが会社所有のデバイスを業務目的で使用している場合であっても、位置情報にプライバシーが保持されるという合理的な期待があるためで

す。合衆国憲法修正第 4 条は、政府による不当な搜索や押収から個人を保護し、電子通信プライバシー法 (ECPA) は、民間人による電子通信の不正な傍受やアクセスを禁止しています。したがって、パトリックは、同意、契約、裁判所命令などの有効な法的根拠がなければ、ジェーンの GPS データを検査することはできません。電話消費者保護法 (A) に従ってジェーンから事前に同意を得ることは関係ありません。この法律は、迷惑電話やテキストメッセージを規制するものであり、位置情報の追跡を規制するものではないためです。評判の良い擁護団体と新しい職場のプライバシーのベスト プラクティスを修正する (B) だけでは十分ではありません。パトリックは、既存の法的義務と契約条件を遵守する必要があります。パトリックは政府を代表して行動しているわけでも、法的要請に応じて行動しているわけでもないため、法執行機関からの召喚状や裁判所命令を取得してジョーンズ ラボに GPS 地理位置情報データを収集するよう指示する必要はありません。ただし、パトリックがそのような法的命令を取得した場合は、法律で禁止されていない限り、それに従い、ジェーンに開示を通知する必要があります。参考資料:

- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.1.2、p. 115-116
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.2.1、p. 118-119
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.2.2、p. 120-121
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.2.3、p. 122-123
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.1、p. 124-125
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.2、p. 126-127
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.3、p. 128-129
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.4、p. 130-131
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.5、p. 132-133
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.6、p. 134-135
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.7、p. 136-137
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.8、p. 138-139
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.9、p. 140-141
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.10、p. 142-143
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.11、p. 144-145
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.12、p. 146-147
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.13、p. 148-149
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.14、p. 150-151
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.15、p. 152-153
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.16、p. 154-155
- * IAPP CIPP/US 学習ガイド、第 4 章、セクション 4.3.17、p. 156-157

最新問題: 23

次のどれが、HIPAA プライバシー ルールに基づく承認要件の例外に該当しないでしょうか。

- A. 公衆衛生活動のために健康情報を公開します。
- B. 児童虐待の報告を提出するために健康情報を開示する。

- C. 医療上の緊急事態を治療するために必要な健康情報を開示する。
- D. サードパーティの請求管理者に支払うために必要な健康情報を開示します。

Answer: C (メッセージを残す)

セクション: (なし)

説明

最新問題: 24

カリフォルニア州の SB 1386 は、米国で最初のこの種の法律で、何を目的としていましたか？

- A. 商業団体に、州住民の個人情報に関するセキュリティデータ侵害の開示を義務付ける
- B. カリフォルニア州で発生した違反について、カリフォルニア州外の居住者に通知することを要求する
- C. インターネットに接続されたサーバーに保存されている機密情報の暗号化を要求する
- D. 不公正で欺瞞的な取引慣行に対する連邦規制の施行を州司法長官に義務付ける

Answer: (解答を表示する)

カリフォルニア州の SB 1386 (カリフォルニア州セキュリティ侵害情報法とも呼ばれる) は、2002 年に制定され、2003 年に発効しました。これは、カリフォルニア州の居住者の個人情報を所有またはライセンスしている商業組織に、暗号化されていないデータが侵害されるセキュリティ侵害が発生した場合にカリフォルニア州居住者に通知することを義務付ける、米国初の法律です。この法律は、個人情報のプライバシーとセキュリティを保護し、個人が個人情報の盗難や詐欺に対する予防措置を講じられるようにすることを目的としています。この法律は、カリフォルニア州で事業を営み、法律で定義されている個人情報を含むコンピューター データを所有またはライセンスしているすべての企業または個人に適用されます。個人情報には、個人のファースト ネームまたはファースト イニシャルと姓、および次の 1 つ以上のデータ要素が含まれます。

社会保障番号、運転免許証番号またはカリフォルニア州身分証明書番号、口座番号、クレジットカードまたはデビットカード番号、および個人の金融口座、医療情報または健康保険情報へのアクセスを許可する必要なセキュリティ コード、アクセス コードまたはパスワードの組み合わせ。この法律は、暗号化された情報、公開されている情報、または連邦、州、または地方政府の記録から合法的に取得された情報には適用されません。この法律では、暗号化されていない個人情報が権限のない人物によって取得された、または取得されたと合理的に考えられるカリフォルニア州の居住者に、システムのセキュリティ侵害を開示することを義務付けています。この開示は、法執行機関の正当な必要性または侵害の範囲を特定してデータ システムの合理的な整合性を回復するために必要な措置に従って、可能な限り迅速に、不当な遅延なく行う必要があります。開示は、法律で指定されているように、書面による通知、電子通知、または代替通知によって行うことができます。また、この法律では、個人または企業が所有していない個人情報を含むコンピュータ化されたデータを保持する場合、その個人情報が権限のない人物によって取得されたか、取得されたと合理的に考えられる場合、データのセキュリティ侵害を発見したら直ちにその情報の所有者またはライセンシーに通知することを義務付けています。また、この法律では、法律違反によって被害を受けた顧客による損害賠

償の民事訴訟を認めており、法律に基づいて利用できる権利と救済策は、相互に、また法律に基づいて利用できるその他の権利と救済策と重複すると規定しています。参考文献:

- * カリフォルニア州上院法案 1386 (2002)
- * カリフォルニア州 SB 1386: プライバシーの保護のために
- * カリフォルニア州セキュリティ侵害情報法とは何ですか?
- * カリフォルニア州、データセキュリティとプライバシーの基準を引き上げ

最新問題: 25

次の州のうち、データブローカーの行為を具体的に規制する法律を可決した最初の州はどれですか?

- A. ワシントン。
- B. カリフォルニア。
- C. バーモント州。
- D. ニューヨーク。

Answer: ([解答を表示する](#))

最新問題: 26

金融機関は、マーケティング目的で消費者情報を非関連第三者と共有できるのはどのような場合ですか?

- A. 顧客にマーケティング手法を開示し、オプトインする機会を与えた後。
- B. 情報共有の慣行を顧客に開示し、顧客にオプトアウトの機会を与えた後。
- C. 顧客にマーケティング手法を開示し、オプトアウトする機会を与えた後。
- D. 情報共有の慣行を顧客に開示し、顧客にオプトインの機会を与えた後。

Answer: B ([メッセージを残す](#))

最新問題: 27

生徒が高校を卒業し、公立の高等教育機関に通っています。どのような条件であれば、学校は生徒の両親の同意なしに教育記録を合法的に開示できますか?

- A. 学生が他の教育機関への転校を申請している場合
- B. 学生が税務上の扶養家族である場合
- C. 学生が停学処分を受ける恐れがある場合
- D. 学生がまだ18歳になっていない場合

Answer: ([解答を表示する](#))

最新問題: 28

保健福祉省 (HHS) 内のどの組織が医療保険の携行性と責任に関する法律 (HIPAA) の「プライバシー規則」を主に施行していますか?

- A. 社会福祉局。
- B. 公衆衛生安全局。
- C. 公民権局。

D. 監察総監室。

Answer: C ([メッセージを残す](#))

最新問題: 29

ドッド・フランク法の重要な意味は次のどれですか？

- A. 金融機関は、ほとんどの種類の顧客記録に対して規定レベルの暗号化を使用する必要があります。
- B. 金融機関は、ダイレクトマーケティングをオプトアウトした顧客への電子メールやその他の広告の送信を停止する必要があります。
- C. 金融機関は顧客の個人情報の機密収集を避けなければならない
- D. 金融機関は顧客が商品やサービスについて理解できるように支援する必要がある

Answer: D ([メッセージを残す](#))

最新問題: 30

シナリオ

次の質問に回答するには、以下を使用してください。

ラリーは、サンライズリンクスでのテレマーケティングの職務、特に上司のエヴァンにますます不満を募らせている。先週、エヴァンが州の Do Not Call リストとそこに載っている人々をあざ笑っているのを耳にした。迷惑をかけたくないと本気で思っているなら、全国 DNC リストに載っているはずだ。それが私たちが従わなければならない唯一のリストだ。サンライズリンクスでは、「電話しないでほしいと言われるまで電話をかけ続ける」。奇妙なことに、エヴァンはテレマーケティング担当者に、受信者が「別の機会に」電話してほしいと頼んだ場合の記録を残すよう要求している。ラリーにとって、これは彼らがまったく電話を受けたくないという明らかな兆候だ。エヴァンはそうは考えていない。

ラリーは、エヴァンの傲慢さが従業員への接し方にも影響していると考えています。米国憲法は米国の労働者を保護しており、ラリーはサンライズリンクスの従業員の権利が定期的に侵害されていると考えています。最初、エヴァンはソーシャルメディアで従業員と交流するなど、友好的に見えました。しかし、エヴァンの政治的な投稿の後、ラリーは、昇進を申し出られるのは同様の所属を持つ従業員だけであることに気づきました。

さらに、ラリーは時々、私的使用の品が入った小包を職場に郵送してもらっています。名前がはっきり記されているにもかかわらず、すでに開封された状態で届いたことが何度かありました。ラリーは、サンライズリンクスでは私的郵便物の開封は一般的であり、エヴァンのリーダーシップの下では憲法修正第 4 条の権利が踏みにじられていると考えています。

ラリーは同僚のセイディーに関する会話を耳にして落胆したこともある。テレマーケティングの電話は品質保証のために定期的に録音されており、セイディーは仕事中は常にプロフェッショナルだが、私的な会話には性的な発言が含まれることがある。ラリーはエヴァンがこれについても笑っているのを聞いたことがある。彼が同僚にこのことを話すと、彼の懸念は肩をすくめるだけで済んだ。同僚は、従業員は入社時に監視されることに同意していると思っていた。個人のデバイスには手を付けていないが、電話、メール、閲覧履歴はすべて監

視対象となっている。実際、ラリーは、外部の会社による覆面調査で不正行為の証拠が見つかり、従業員が解雇された事例を1件知っている。その従業員は会社から盗んだのかもしれないが、エヴァンは何かおかしいと最初に疑った時点で当局に連絡すればよかったのだ。ラリーは行動を起こしたいと思っていますが、どのように進めればよいかわかりません。どの行為がエヴァンの潜入捜査を許可するのでしょうか？

- A. 内部告発者保護法
- B. 全国労働関係法 (NLRA)
- C. 保存通信法 (SCA)
- D. 公正かつ正確な信用取引法 (FACTA)

Answer: B (メッセージを残す)

最新問題: 31

カリフォルニア州の SB 1386 は、米国で最初のこの種の法律で、何を目的としていましたか？

- A. 商業団体に、州住民の個人情報に関するセキュリティデータ侵害の開示を義務付ける
- B. カリフォルニア州で発生した違反について、カリフォルニア州外の居住者に通知することを要求する
- C. インターネットに接続されたサーバーに保存されている機密情報の暗号化を要求する
- D. 不公正で欺瞞的な取引慣行に対する連邦規制の施行を州司法長官に義務付ける

Answer: A (メッセージを残す)

説明/参照: <https://corporate.findlaw.com/law-library/california-raises-the-bar-on-data-security-and-privacy.html>

有効な **CIPP-US** 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集！ GoShiken.com が最新の **CIPP-US** 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (228**30%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 32

公民権法、妊娠差別禁止法、アメリカ障害者法、年齢差別禁止法、同一賃金法の共通点は何でしょうか？

- A. 従業員が個人情報を利用する際に、雇用主は特定の階級に対して差別を行わないことが義務付けられている。
- B. 雇用主は特定の従業員に対して合理的な配慮を提供することが義務付けられている
- C. 個人情報に関する問い合わせを制限することで、特定の従業員のプライバシー保護を実現している

D. 雇用主が特定のクラスに属する従業員の個人情報を使用したり開示したりすることを許可する

Answer: ([解答を表示する](#))

公民権法、妊娠差別禁止法、アメリカ障害者法、年齢差別禁止法、同一賃金法はすべて、人種、性別、障害、年齢、賃金などの特定の保護特性に基づく雇用差別を禁止する連邦法です1234 これらの法律は、保護対象ステータスを明らかにしたり、差別目的に使用されたりする可能性のある個人情報に関する問い合わせを制限することで、特定の従業員のプライバシー保護も保証します。例:

* 1964 年公民権法では、それが職業上の正当な資格でない限り、雇用者が雇用前に人種、肌の色、宗教、性別、または国籍に基づく優先、制限、または仕様を表明する質問をすることを禁止しています。

* 1964 年公民権法を改正した 1978 年妊娠差別禁止法では、職務遂行能力に関係しない限り、雇用者が妊娠しているか、妊娠する予定があるかどうかについて雇用前に質問することを雇用主に禁止しています。

* 1990 年のアメリカ障害者法では、合理的配慮の有無にかかわらず職務の必須機能を遂行する能力に関係しない限り、雇用者が障害を持っているかどうか、または障害の性質や重症度について雇用前に質問することを雇用主が禁止しています。

* 1967 年の雇用年齢差別禁止法では、正当な職業資格または合法的な積極的差別是正措置計画に関連する場合を除き、雇用者が求職者の年齢について雇用前に質問することを禁止しています。

* 1963 年の男女賃金平等法では、応募者の給与を決定する以外の合法的な目的で行われる場合を除き、雇用主が応募者の給与履歴について雇用前に問い合わせることを禁止しています。

オプション A は不正解です。なぜなら、これらの法律は、従業員が個人情報を使用する際に雇用主が特定のクラスに対して差別しないことを義務付けていないからです。むしろ、雇用、解雇、給与、昇進、研修、福利厚生など、雇用のあらゆる側面において雇用主が特定のクラスに対して差別しないことを義務付けています。1234 従業員による個人情報の使用は、他のプライバシー法やポリシーの対象となることはありますが、これらの法律では直接取り上げられていません。

オプション B は誤りです。これらの法律では、雇用主が特定の従業員に合理的配慮を提供することを義務付けていません。むしろ、アメリカ障害者法と妊娠差別禁止法のみが、雇用主に過度の負担をかけない限り、適格な障害者と妊娠、出産、または関連する病状に関連する制限のある労働者に合理的配慮を提供することを義務付けています。その他の法律には同様の要件はありませんが、雇用主が特定の従業員に平等な機会を拒否することを禁止している場合があります。

オプション C が正解です。なぜなら、これらの法律は、上で説明したように、保護されているステータスを明らかにしたり、差別目的で使用される可能性のある個人情報に関する問い合わせを制限することで、特定の従業員のプライバシー保護を可能にしているからです。

オプション D は不正解です。これらの法律では、特定のクラスに属する従業員に関する個人情報を雇用主が使用または開示することは許可されていません。むしろ、これらの法律では、例外が適用されない限り、雇用主がこれらの法律で保護されている個人情報を違法または差別的な目的で使用または開示することは一般的に禁止されています。たとえば、雇用主は、報告要件の遵守、給付の管理、調査の実施など、正当なビジネス上の理由でそのような情報を使用または開示できます。

参照資料: 1: 同一賃金および報酬差別に関する事実 2: 妊娠差別および妊娠関連障害差別 | 米国雇用機会均等委員会 3: 規制、ガイダンス、ポリシー | 機会均等ガイダンス | OEEOWE 4: 年齢差別 | 米国雇用機会均等委員会: 雇用前調査および健康上の質問と検査 | 米国雇用機会均等委員会: 従業員の医療情報 | 米国雇用機会均等委員会: 従業員のプライバシー権 | 米国労働省: 1964 年公民権法第 7 条 | 米国雇用機会均等委員会: ファクトシート: 妊娠差別 | 米国雇用機会均等委員会: アメリカ障害者法: 中小企業向け入門書: 1967 年雇用における年齢差別禁止法 | 米国雇用機会均等委員会: 1963 年同一賃金法 | 米国雇用機会均等委員会

最新問題: 33

グラム・リーチ・ブライリー法 (GLBA) に基づいて銀行は何をする必要がありますか?

- A. ユーザーの嗜好に対する満足度に関する消費者調査を毎年実施する
- B. 指定された時間枠内でユーザー設定の変更要求を処理する
- C. 消費者にテレマーケティングの電話を受け取らないよう選択する機会を提供する
- D. 個人情報を提携関係のない第三者に譲渡して第三者自身の使用に供する前に、オプトアウトを提案する

Answer: D (メッセージを残す)

説明/参照: <https://www.investopedia.com/terms/g/glba.asp>

最新問題: 34

1988 年のビデオ プライバシー保護法では、次のどれが制限されましたか?

- A. オーディオビジュアル資料の購入記録は開示される可能性があるか
- B. 著作権のあるオーディオビジュアル素材のダウンロードが許可されている場合
- C. ユーザーのオンライン動画コンテンツの視聴を監視できる場合
- D. ビデオやビデオゲームの広告のターゲットとなる可能性のある人

Answer: (解答を表示する)

VPPA は、ビデオ テープ サービス プロバイダーの消費者に関する個人識別情報 (PII) の不正な開示を防止するために制定されました。PII には、ビデオ テープ サービス プロバイダーから特定のビデオ素材またはサービスを要求または取得した人物を特定する情報が含まれます。VPPA は、消費者の書面による同意がある場合、または法執行令状、召喚状、裁判所命令に従う場合など、特定の限定された状況を除き、そのような開示を禁止しています。VPPA では、消費者の名前と住所の開示も許可されていますが、消費者がそのような開示を拒否しない限り、ビデオ テープやその他のオーディオ ビジュアル素材のタイトル、説明、または主題は許可されていません。その他のオプション (B、C、および D) は、VPPA によって制限されていません。参考資料:

* ビデオプライバシー保護法 - Wikipedia

* 18 US Code § 2710 - ビデオテープのレンタルまたは販売記録の不正開示 | US Code | 米国法 | LII / 法律情報研究所

* IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第 3 章: 連邦プライバシー法および規制、セクション 3.5: ビデオ プライバシー保護法 (VPPA)

最新問題: 35

公正かつ正確な信用取引法 (FACTA) は公正信用報告法 (FCRA) をどのように改正しましたか?

- A. 消費者レポート」の定義を拡大し、従業員の調査に関する通信も含めるようにした。
- B. 消費者データを不正アクセスを防止する方法で処分する組織の義務が強化された。
- C. 消費者レポートを取得する目的は、従業員の信用力の検討のみであると規定されている。
- D. 内部調査の目的で消費者レポートを要求する前に、雇用主が従業員の同意を得ることを義務付けた。

Answer: ([解答を表示する](#))

FACTA は、FCRA に新しいセクションを追加し、消費者レポートから得た消費者情報または消費者情報の編集物をビジネス目的で保持または保有するすべての人に、そのような情報または編集物を適切に処分することを義務付けました。この条項の目的は、消費者情報の不適切な処分によって生じる個人情報の盗難やその他の消費者被害のリスクを軽減することです。FTC およびその他の連邦機関は、この条項を実施する規則を発行し、対象となる事業者が消費者情報の安全な処分を確実にするために講じなければならない合理的な措置 (情報を焼却、粉碎、細断、消去、または読み取り不能または判読不能にするためのその他の変更など) を規定しています (16 CFR § 682.3)。参照: 1、2、3

最新問題: 36

特定の連邦執行機関の目的を正確に説明しているものはどれですか?

- A. 米国国立標準技術研究所 (NIST) は、司法省 (DOJ) がすべての営利組織に対して強制できるプライバシー標準を確立しました。
- B. サイバーセキュリティおよびインフラストラクチャセキュリティ庁 (CISA) には、Web サイトまたはその他のオンライン サービスで個人情報が適切に保護されていない組織に対して民事執行措置を講じる権限があります。
- C. 連邦通信委員会 (FCC) は、インターネット上のプライバシー慣行を規制し、Web サイトに掲載されたプライバシー開示に関する違反を強制します。
- D. 連邦取引委員会 (FTC) は、通常、FTC 法に基づいて不公正または欺瞞的なプライバシー慣行に対処する最も広範な権限を持つ機関として認識されています。

Answer: D ([メッセージを残す](#))

FTC は、米国におけるプライバシーおよびデータ セキュリティ法の執行を担当する主要な連邦機関です。FTC は、消費者から個人情報を収集、使用、または共有するほとんどの商業団体に対して広範な管轄権を持っています。FTC 法は、商業における、または商業に影響を与え

る不公正または欺瞞的な行為または慣行を禁止しており、これには不公正または欺瞞的なプライバシー慣行が含まれます。FTC は、自社のプライバシー ポリシーに違反する企業、消費者に適切な通知または選択肢を提供しない企業、不公正または有害なデータ慣行に従事する企業、または消費者のプライバシーに関する合理的な期待に反する企業に対して、執行措置を講じることができます。FTC は、プライバシーおよびデータ セキュリティの問題に関する規則、ガイドライン、レポートを発行するほか、調査、ワークショップ、教育キャンペーンを実施することもできます。参考資料:

- * IAPP CIPP/US 知識体系、セクション IA1.a
- * IAPP CIPP/US 教科書、第 1 章、9-12 ページ
- * FTCのプライバシーとセキュリティの施行

最新問題: 37

FERPA によれば、学校はどのような場合に生徒の同意なしに記録を開示できるのでしょうか?

- A. 開示が、学生が入学を希望する学校に成績証明書を提供することである場合
- B. 開示によって学生の学生番号が明らかにならない場合
- C. 開示が第三者への電子メールを通じて行われえない場合
- D. 学生の健康管理に携わる医療従事者への開示の場合

Answer: ([解答を表示する](#))

最新問題: 38

次の州のうち、生体認証データの収集を具体的に規制する法律を制定した最初の州はどれですか?

- A. ワシントン。
- B. テキサス。
- C. カリフォルニア。
- D. イリノイ州。

Answer: D ([メッセージを残す](#))

最新問題: 39

シナリオ

次の質問に回答するには、以下を使用してください。

あなたは、米国 A 州の大都市にある大規模病院、HealthCo の最高プライバシー責任者です。HealthCo は HIPAA の対象事業体であり、100,000 人以上の患者に医療サービスを提供しています。サードパーティのクラウド コンピューティング サービス プロバイダーである CloudHealth は、HealthCo に代わってこれらの個人の電子保護医療情報 (ePHI) を保存および管理しています。CloudHealth はデータを状態 B に保存します。HealthCo と CloudHealth とのビジネス アソシエート契約 (BAA) の一環として、HealthCo は CloudHealth に対し、データを適切に保護するために業界標準の暗号化手法を含むセキュリティ対策を実施することを要求しています。しかし、HealthCo は契約締結前に

CloudHealth に対してデューデリジェンスを実施しておらず、CloudHealth のセキュリティ対策の監査も実施していません。

CloudHealth の従業員が最近フィッシング攻撃の被害者になりました。従業員が不審なメールのリンクをうっかりクリックしたため、HealthCo の患者 10,000 人以上の PHI が侵害され、その後、その情報がオンラインで公開されました。HealthCo のサイバーセキュリティチームは、犯人が他の病院に対して同様の攻撃を仕掛けた既知のハッカーであることをすぐに特定しました。この攻撃では、著名人や政治家などの公人の PHI が漏洩しました。

調査の過程で、HealthCo は、CloudHealth が契約条件に従って PHI を暗号化していなかったことを発見しました。さらに、CloudHealth は従業員にプライバシーやセキュリティに関するトレーニングを提供していませんでした。法執行機関は、HealthCo に対し、侵害に関する調査報告書と影響を受けた個人の PHI のコピーを提供するよう要求しました。

侵害の影響を受けた患者は、HealthCo 社が患者の ePHI を適切に保護しなかったため、漏洩したデータによって患者が多大な損害を被ったと主張して同社を訴えました。患者の弁護士は、侵害で漏洩した ePHI に関する証拠開示請求を提出しました。

米国保健福祉省 (HHS) が HealthCo に罰金を課す可能性がある最も重要な理由は何ですか？

- A. CloudHealthはePHIを暗号化しなかったことでHealthCoとの契約に違反したため
- B. HIPAAでは、この規模のデータ侵害が発生した場合に罰金を科すことが義務付けられているため
- C. HealthCoはCloudHealthのセキュリティ対策を検証または監視するためのデューデリジェンスを実施しなかったため
- D. HealthCoは、ePHIを保護するためにCloudHealthに適切な物理的および管理的措置を講じることを要求しなかったため

Answer: ([解答を表示する](#))

最新問題: 40

米国の民間部門の職場監視について最もよく説明されているのは次のどれですか？

- A. 雇用主は従業員を監視する広範な権限を持っている
- B. 民事訴訟の判決により、従業員の監視が厳しく制限されている
- C. ほとんどの従業員は米国憲法によって職場の監視から保護されている
- D. 米国連邦法では、監視は必要な業界のみに制限されている。

Answer: ([解答を表示する](#))

最新問題: 41

サラさんはカリフォルニア州サンフランシスコに住んでいます。迷惑な商業メールが急増していることから、5,000 万人以上のユーザーを抱える大手ソーシャルメディアプラットフォームがサラさんの個人情報を大量に収集しているのではないかと考えています。このプラットフォームを運営する会社はニューヨークとフランスに拠点を置いています。

なぜサラはソーシャルメディアプラットフォームに対して、彼女について収集された個人情報を削除するよう要求する権利があるのでしょうか？

- A. ヨーロッパに拠点を置く企業は、データ主体の削除要求への対応を含め、世界的に一般データ保護規則に準拠する必要があります。
- B. FTC 法第 5 条に基づき、連邦取引委員会は、個人の個人情報の削除要求を拒否することは不公正な行為に当たると判断しました。
- C. カリフォルニア州消費者プライバシー法により、サラは自分の個人情報の削除を要求する権利を有します。
- D. ニューヨーク州の「ハッキングを阻止し、電子データ セキュリティを強化する」(SHIELD) 法では、ニューヨーク州の管轄下にある企業は、要求に応じて顧客の個人情報を削除することが義務付けられています。

Answer: (解答を表示する)

正解は C です。カリフォルニア州消費者プライバシー法 (CCPA) は、カリフォルニア州の住民に、企業が収集した個人情報の削除を要求する権利を与える州のプライバシー法であるためです。CCPA は、収益、データ量、またはデータ共有の特定の基準を満たしている限り、企業の所在地に関係なく、カリフォルニア州の住民から個人情報を収集するすべての企業に適用されます。したがって、サラが使用するソーシャル メディア プラットフォームは CCPA の対象であり、例外が適用されない限り、サラの削除要求を尊重する必要があります。CCPA では、企業に対して、データ収集および使用方法について消費者に通知し、選択肢を提供すること、および消費者の要求に 45 日以内に応答することを義務付けています。

他の回答は、以下の理由で不正解です。

* A は不正解です。一般データ保護規則 (GDPR) は、データ管理者またはデータ処理者の所在地に関係なく、EU 内の個人の個人データの処理に適用される欧州連合のプライバシー法です。ただし、処理がそのような個人への商品またはサービスの提供、または EU 内での行動の監視に関連するものでない限り、GDPR は EU 外の個人の個人データの処理には適用されません。したがって、サラは EU 内におらず、ソーシャル メディア プラットフォームは EU 内でサラをターゲットにしたり追跡したりしていないため、GDPR はサラの個人データには適用されません。

* B は誤りです。FTC 法第 5 条は、商取引における、または商取引に影響を与える不公正または欺瞞的な行為や慣行を禁止する連邦法です。FTC は、第 5 条の権限を使用して、自社のプライバシー ポリシーに違反したり、データ慣行を偽ったり、消費者データを不正アクセスや開示から保護しなかったりする企業に対して、プライバシーとデータセキュリティの基準を強制してきました。ただし、FTC は、要求に応じて個人の個人情報を削除することを拒否すること自体が不公正な慣行であるとは判断していません。ただし、その拒否が企業のプライバシー ポリシーや表明と矛盾する場合、または消費者に合理的に回避できない、または相殺利益によって上回らない重大な損害を与える場合は除きます。

* D は不正解です。ニューヨーク州 SHIELD 法は、ニューヨーク州居住者の個人情報を含むコンピューター データを所有またはライセンスする個人または企業に、データ侵害通知およびデータ セキュリティ要件を課す州法です。SHIELD 法は、ニューヨーク州居住者に個人情報の削除を要求する権利を与えておらず、ニューヨーク州居住者の個人情報を収集または保持していない企業には適用されません。したがって、サラはニューヨーク州居住者ではなく、

ソーシャルメディアプラットフォームは SHIELD 法で定義されている彼女の個人情報を保有していない可能性があるため、サラの個人データには SHIELD 法は適用されません。参考文献:

* Peter P. Swire、DeBrae Kennedy-Mayo 著 『米国民間部門のプライバシー』第 3 版、第 7 章、セクション 7.2.1、183-186 ページ。

* Mike Chapple および Joe Shelley 著 『APP CIPP/US 認定情報プライバシー専門家学習ガイド』、第 7 章、セクション 7.2、217 ~ 219 ページ。

最新問題: 42

1974 年の家族教育権利とプライバシー法 (FERPA) に違反する行為はどれですか？

A. K-12 評価ベンダーは、学校から生徒の故郷についての署名入りのエッセイを入手し、公開用のサンプルとして使用します。

B. 大学は、名前、出身地、電子メールアドレス、専攻を含む学生名簿を公開しています。

C. 新聞には、四半期ごとの優秀者名簿に載った生徒の名前、学年、出身地が掲載される。

D. 大学警察は学生の地元警察に逮捕報告書を提出し、地元警察は同様の犯罪を疑っている。

Answer: [\(解答を表示する\)](#)

1974 年の家族教育権利とプライバシー法 (FERPA) は、学生の教育記録のプライバシーを保護する連邦法です。FERPA は、一部の例外を除き、保護者または資格のある学生に教育記録へのアクセス、修正、開示の制御の権利を与えています。学校は、例外が適用されない限り、教育記録から個人を特定できる情報を開示する前に、保護者または資格のある学生から書面による同意を得る必要があります。123 オプション A は、教育記録から学生の個人を特定できる情報 (PII) を同意なしに開示することを伴うため、FERPA に違反しています。学生が自分の故郷について書いた署名入りのエッセイは、学生に直接関連し、学校によって保管されているため、FERPA の下では教育記録とみなされます。12 K-

12 評価ベンダーは、正当な教育上の利益を有する学校関係者ではなく、同意なしの開示を許可する例外のいずれにも該当しません。12 したがって、学校は、エッセイをベンダーに提供して公開する前に、生徒（生徒が未成年の場合は保護者）の書面による同意を得る必要があります。

オプション B は、ディレクトリ情報の開示を伴うため、FERPA に違反しません。ディレクトリ情報は、FERPA では PII とは見なされません。ディレクトリ情報とは、名前、住所、電話番号、電子メールアドレス、専攻など、開示されても一般的に有害またはプライバシーの侵害とは見なされない情報です¹²。学校は、親または資格のある学生がそのような開示をオプトアウトしない限り、同意なしにディレクトリ情報を開示できます¹²。ただし、学校は、指定するディレクトリ情報の種類とオプトアウトする権利を毎年親と資格のある学生に通知する必要があります¹²。オプション C は、教育記録の一部ではない情報の開示を伴うため、FERPA に違反しません。FERPA は、学生に直接関連し、学校または学校に代わって行動する当事者によって保持されている教育記録にのみ適用されます¹²。四半期ごとの優等生名簿に載った学生の名前、学年、出身地を新聞が公表することは、教育記録に基づくものではなく、新聞独

自の情報源と報道に基づいています。したがって、FERPA はそのような開示を禁止していません。

オプション D は、同意なしの開示を許可する例外に基づく情報開示を伴うため、FERPA に違反しません。FERPA では、学校が裁判所命令または合法的に発行された召喚状に従うため、または健康や安全上の緊急事態に関連して適切な当局に、同意なしに教育記録または教育記録の PII を開示することを許可しています¹²³ 大学警察が召喚状に応じて、または学生または他の人への深刻な脅威を防ぐために、学生の地元警察に逮捕報告書を提供する場合、FERPA に違反していません。

参照: 1: 家族教育の権利とプライバシー法 - Wikipedia 2: 家族教育の権利とプライバシー法 (FERPA) | CDC 3: FERPA とは? | 学生のプライバシーの保護 - ed

最新問題: 43

シナリオ

次の質問に回答するには、以下を使用してください。

あなたは、米国州 A の大都市にある主要病院 HealthCo の最高プライバシー責任者です。HealthCo は HIPAA の対象事業体であり、100,000 人以上の患者に医療サービスを提供しています。サードパーティのクラウド コンピューティング サービス プロバイダーである CloudHealth は、HealthCo に代わってこれらの個人の電子保護医療情報 (ePHI) を保存および管理しています。CloudHealth はデータを州 B に保存します。HealthCo と CloudHealth とのビジネス アソシエート契約 (BAA) の一環として、HealthCo はデータを適切に保護するために、業界標準の暗号化手法を含むセキュリティ対策を CloudHealth に実装することを要求しています。

しかし、HealthCo は契約締結前に CloudHealth に対するデューデリジェンスを実施しておらず、CloudHealth のセキュリティ対策の監査も実施していません。

CloudHealth の従業員が最近フィッシング攻撃の被害者になりました。従業員が不審なメールのリンクをうっかりクリックしたため、HealthCo の患者 10,000 人以上の PHI が侵害され、その後、その情報がオンラインで公開されました。HealthCo のサイバーセキュリティチームは、犯人が他の病院に対して同様の攻撃を仕掛けた既知のハッカーであることをすぐに特定しました。この攻撃では、著名人や政治家などの公人の PHI が漏洩しました。

調査の過程で、HealthCo は、CloudHealth が契約条件に従って PHI を暗号化していなかったことを発見しました。さらに、CloudHealth は従業員にプライバシーやセキュリティに関するトレーニングを提供していませんでした。法執行機関は、HealthCo に対し、侵害に関する調査報告書と影響を受けた個人の PHI のコピーを提供するよう要求しました。

侵害の影響を受けた患者は、HealthCo 社が患者の ePHI を適切に保護しなかったため、漏洩したデータによって患者が多大な損害を被ったと主張して同社を訴えました。患者の弁護士は、侵害で漏洩した ePHI に関する証拠開示請求を提出しました。

弁護士の証拠開示要求に対する HealthCo の最善の対応は次のどれでしょうか？

A. HIPAA のプライバシー規則では支払い、治療、または医療業務の目的のみに開示が許可されているため、要求を拒否します。

- B. 限定的保護命令などの満足のいく保証の要求に応じる
- C. 侵害された患者の記録をすべて原告の弁護士に引き渡す
- D. 原告に関する部分のみ編集した文書で回答する

Answer: B (メッセージを残す)

HIPAA プライバシー規則は、個人の医療記録やその他の個人を特定できる健康情報 (総称して「保護された健康情報」と定義) を保護するための国家基準を確立し、医療保険、医療情報センター、および特定の医療取引を電子的に行う医療提供者 (総称して「対象事業体」と定義) に適用されます¹。この規則は、保護された健康情報のプライバシーを保護するための適切な保護措置を要求し、個人の許可なしにそのような情報を使用および開示できる場合の制限と条件を設定します¹。この規則はまた、個人に保護された健康情報に関する権利を与えており、これには、健康記録を調べてコピーを取得する権利、対象事業体に電子健康記録内の保護された健康情報の電子コピーを第三者に送信するよう指示する権利、および訂正を要求する権利が含まれます¹。HIPAA プライバシー規則は、対象事業体が、裁判所命令、召喚状、証拠開示請求、またはその他の合法的なプロセスに応じて訴訟のために保護された健康情報を開示することを許可しています。ただし、司法および行政のための開示に関する 45 CFR 164.512 (e) の適用要件を満たす必要があります。手続きが満たされている² これらの要件には以下が含まれます。

* 裁判所命令または行政裁判所命令に応じて、対象事業体は、当該命令によって明示的に許可された保護された健康情報のみを開示することができる²

* 裁判所命令や行政審判所命令を伴わない召喚状、証拠開示請求、その他の合法的な手続きに応じて、対象事業体は、情報を求める当事者が、情報の対象である個人に要求が通知されたことを確認するために合理的な努力を払ったこと、または情報を求める当事者が適格な保護命令を確保するために合理的な努力を払ったことについての十分な保証を受けなければならない²

* 限定保護命令とは、裁判所または行政裁判所の命令、または訴訟または行政手続きの当事者による合意であり、当事者が保護対象健康情報を、その情報が要求された訴訟または手続き以外の目的で使用または開示することを禁止し、訴訟または手続きの終了時に保護対象健康情報 (作成されたすべてのコピーを含む) を対象事業体に返却するか破棄することを要求するものです。² オプション A は、HIPAA プライバシー規則では支払い、治療、または医療業務のための開示のみが許可されているわけではないため、正しくありません。この規則では、適用される条件と制限が満たされている限り、公衆衛生、研究、法執行、司法手続きおよび行政手続きなどの他の目的での開示も許可されています。¹ オプション B は、司法手続きおよび行政手続きのための開示に関する HIPAA プライバシー規則の要件と一致しているため、正解です。適格保護命令などの十分な保証の要求に応じることで、HealthCo は、保護された健康情報が訴訟のみに使用され、その後返却または破棄されることを保証しています² オプション C は、司法手続きおよび行政手続きのための開示に関する HIPAA プライバシー規則の要件と一致していないため、正しくありません。侵害された患者の記録をすべて原告の弁護士に引き渡すことで、HealthCo は必要以上の情報を開示し、訴訟の当事者ではない他の個人のプライバシー権を侵害する可能性があります² オプション D は、司法手続きおよび行

政手続きのための開示に関する HIPAA プライバシー ルールの要件と一致していないため、正しくありません。原告に関連する部分のみを編集した文書で応じることで、HealthCo は、保護された健康情報が訴訟のみに使用され、その後返却または破棄されることについて、十分な保証を提供していません² 参照: 1: HIPAA プライバシー ルールの概要 | HHS.gov 2: 対象事業体は保護された健康情報を訴訟のために使用または開示できますか? | HHS.gov

最新問題: 44

連邦法では、13 歳未満の未成年者の個人情報を収集するための次の要件のうちどれが定められていますか?

- A. 未成年者の個人情報をオフラインで収集する前に、親または保護者の同意を得ること (例: オンラインでの同意の要件も満たす、対面での同意など)が必要です。
- B. 未成年者にインターネットの使用を許可する場合など、未成年者の個人情報をオンラインで収集する前に、未成年者の親または保護者からの暗黙の同意を得ること。
- C. 未成年者の親または保護者からの暗黙の同意、または未成年者からの積極的な同意。
- D. 未成年者の個人情報をオンラインで収集する前に、未成年者の親または保護者の明示的な同意を得ること。

Answer: D (メッセージを残す)

児童オンラインプライバシー保護法 (COPPA) は、13 歳未満の児童からの個人情報のオンライン収集と使用を規制する連邦法です。COPPA では、児童向けの Web サイトやオンラインサービスの運営者、または児童から故意に個人情報を収集する Web サイトやオンラインサービスの運営者に対し、そのような情報を収集、使用、開示する前に、検証可能な保護者の同意を得ることを義務付けています。検証可能な保護者の同意とは、児童から個人情報を収集する前に、児童の保護者が運営者の情報慣行について通知を受け、その慣行に同意することを保証する、あらゆる合理的な努力 (利用可能なテクノロジーを考慮) を意味します。COPPA では、保護者に児童の情報へのアクセスを提供すること、合理的なセキュリティ対策を維持すること、データ保持を制限することなど、運営者にその他の義務も課しています。参考文献: COPPA、IAPP CIPP/US 学習ガイド、第 2 章、セクション

2.3.1

最新問題: 45

米国の州の半数以上がテレマーケティング業者に次のどれを義務付けていますか?

- A. 通話の始めに自己紹介をする
- B. 潜在顧客から書面による同意を得る
- C. 事業を行う前に州に登録します。
- D. 顧客取引に関する書面による契約を提供する

Answer: C (メッセージを残す)

米国の半数以上の州では、テレマーケティング業者がテレマーケティング活動を行う前に州に登録することを義務付けています。これらの登録要件は、詐欺や不正行為を防止するためにテレマーケティング行為を規制することを目的とした州レベルの消費者保護法の一部です。

州登録が必要な理由:

- * テレマーケティング登録要件により、各州は管轄区域内で営業するテレマーケティング業者を監視および規制できます。
- * 登録により、テレマーケティング業者は「電話禁止」リスト規制や詐欺行為の禁止など、州固有の規則に準拠することが保証されます。
- * フロリダ州、ニューヨーク州、カリフォルニア州などの州は、テレマーケティング登録法を制定している管轄区域の例です。

オプションの説明:

- * A. 通話の冒頭で自己紹介をする: これは連邦取引委員会 (FTC) のテレマーケティング販売規則 (TSR) の要件ですが、州の要件に固有のものではありません。
- * B. 潜在顧客から書面による同意を得る: 同意を得ることは特定の状況では必要となる場合がありますが (例: 自動ダイヤル通話に対する電話消費者保護法 (TCPA) に基づく)、州レベルで最も一般的な要件ではありません。
- * C. 事業を行う前に州に登録する: これは正解です。州への登録は、州法に基づくテレマーケティング業者に対する最も一般的な要件の1つです。
- * D. 顧客との取引について書面による契約を提供する: テレマーケティングでは書面による契約が必ずしも必要というわけではありません。これは、販売される製品またはサービスの種類によって異なります。

CIPP/US 資料からの参照:

- * FTC テレマーケティング販売規則 (TSR): 一般的なテレマーケティング規則を網羅していますが、登録などの州固有の追加要件も考慮しています。
- * 州のテレマーケティング法: 例としては、州の登録を必要とするフロリダ州のテレマーケティング法が挙げられます。

最新問題: 46

USA FREEDOM法ではどのような行為が認められていないのでしょうか?

- A. 政府が徘徊者をターゲットにすることを可能にする緊急例外
- B. テロへの物質的支援に対する最高刑の引き上げ
- C. 移動盗聴の有効期限の延長
- D. 電話データとインターネットメタデータの一括収集

Answer: D (メッセージを残す)

USA FREEDOM法は、米国の監視慣行を改革するために2015年に制定された法律である。政府。この法律は、米国愛国者法第 215 条の権限に基づき国家安全保障局 (NSA) が電話記録とインターネット データを大量に収集していたというエドワード スノーデンの暴露に対する対応として制定されました。USA FREEDOM 法は、NSA による電話データとインターネット メタデータの大量収集を終了し、代わりに政府が通信プロバイダーからそのようなデータにアクセスするには外国情報監視裁判所 (FISC) から特定の命令を取得することを義務付けました。この法律では、以下の行為も許可されました。

- * 政府が徘徊者をターゲットにすることを許可する緊急例外: 法律では、死亡または重大な身体的危害の脅威を伴う緊急事態が発生した場合、裁判所の命令なしに、米国人の電話番号ま

たはIDを使用している米国人以外の人物を政府が一時的にターゲットにすることが許可されています。政府は監視を継続するために7日以内に裁判所命令を取得する必要があります。

* テロへの物質的支援に対する最高刑の引き上げ: この法律により、外国のテロ組織に物質的支援または資源を提供した場合の最長刑期が15年から20年に引き上げられます。

* 移動盗聴の期限延長: この法律は、米国愛国者法の移動盗聴規定の期限を延長する。この規定により、政府は、デバイスや場所を特定することなく、デバイスや場所を変更するターゲットを監視するために、FISCから単一の命令を取得することができる。この法律は、期限を2015年6月1日から12月15日に延長する。

2019年. 参考文献:

* 米国自由法

* USA FREEDOM法の概要

* USA FREEDOM法に関するよくある質問

有効な **CIPP-US** 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集! GoShiken.com が最新の **CIPP-US** 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (22830%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 47

シナリオ

次の質問に回答するには以下を使用してください

大手小売店で顧客の個人情報と財務情報を含むデータ侵害が発生したとき、会社の役員たちは衝撃を受けました。しかし、同社のプライバシーアナリストであり、自身も個人情報盗難の被害者であるロベルタは衝撃を受けませんでした。侵害が発生する前、彼女は役員向けのプライバシープログラムレポートに取り組んでいました。会社が組織全体でデータを共有し、処理する方法が大きな懸念事項でした。顧客情報へのアクセスに関する適切なルールも、古くなったデータを消去および破棄する手順もありませんでした。ロベルタは調査の中で、下級従業員でさえ会社のすべての顧客データ(財務記録を含む)にアクセスでき、1980年代にさかのぼる古い顧客データがまだ会社に残っていることを発見しました。

彼女の報告書では、3つの主要な改革を推奨しています。まず、必要に応じてアクセスを許可すること。つまり、従業員が顧客情報にアクセスできるのは、業務に関連するデータのみ制限するということです。次に、顧客の財務情報(クレジットカード番号や銀行口座番号など)を機密性の低い情報とは別に保管するための、非常に安全なデータベースを作成します。最後に、古くなった顧客情報を特定し、安全に廃棄するプロセスを作成します。

侵害が発生したとき、同社の幹部はロベルタを会議に招集し、彼女は報告書で推奨事項を提示しました。ロベルタは、同社が全国規模の顧客基盤を持つということは、関連するすべての

州の侵害通知法に準拠する必要があることを説明しました。ロベルタの指導のおかげで、同社は州の侵害通知法で定められた特定の時間枠内で迅速に顧客に通知することができました。

その後すぐに、役員らはロベルタが報告書で推奨したプライバシー プログラムの変更を承認しました。これらの変更により、またプライバシーとセキュリティがすべての従業員の責任とみなされるようになったことにより、プライバシー プログラムははるかに効果的になりました。

侵害が発生する前に、リスクを軽減するために会社ができることは何だったでしょうか？

- A. 顧客情報にアクセスするための包括的なポリシーを実装しました。
- B. 会社のネットワークを危険にさらす可能性のある、セキュリティに対する継続的な脅威を探しました。
- C. オプトイン方式を使用して情報を取得するというプライバシー ポリシーの約束を守りました。
- D. 組織全体および第三者にユーザーの設定の変更要求を伝えました。

Answer: ([解答を表示する](#))

最新問題: 48

シナリオ

次の質問に回答するには以下を使用してください

ノアはお金の管理に関わる新しい仕事に就こうとしています。彼の個人信用格付けは低いですが、過去 2 年間で財務上の判断は改善されました。

ノアは、最近、採用候補者の 1 人であるアーニズ エンポリウムから電話を受け、採用されなかったことを知らされました。応募プロセスの一環として、ノアは、採用候補者が消費者信用情報機関 (CRA) に信用レポートを請求することを許可する同意書に署名しました。ノアは、レポートが採用のチャンスを損ねたと考えていますが、信用のせいで採用されなかったかどうかは永遠にわからないと考えています。しかし、ノアはこの特定の職に就けなかったことにいくらかほっとしています。面接を受けた店舗がひどく乱雑だったことに気づいたのです。信用レポートがまだオフィスに無防備に置かれているのではないかと想像しています。

2 日前、ノアはサムズ マーケットでの職に就くために別の面接を受けました。面接官はノアに、信用報告書が採用決定の要因になると伝えました。ノアは、応募したときにこのことについて書類で何も知らなかったため、驚きました。

いずれにせよ、ノアの信用が雇用に及ぼす影響は、特に信用を高めるために一生懸命努力してきただけに、彼を悩ませています。ノアは 15 年前に最悪の金銭的決断を下し、それが破産に至りました。これらは彼が若い頃に下した決断であり、当時の負債の大半は学生ローン、クレジットカードの負債、および未払いの請求書数件で構成されていました。ノアはこれらすべてを今も返済中です。彼は 15 年前の決断が今でも影響を及ぼしているとよく嘆きます。さらに、ノアは大手銀行での投資経験が彼の経済的な問題の一因になったかもしれないと感じています。2007 年、借金返済の資金を稼ぐために、ノアは大手投資会社のカスタマーサー

ビス担当者に相談したところ、株の購入を勧められました。リスクを理解しないまま、ノアは同意しました。残念ながら、ノアは多額のお金を失いました。

お金を失った後、ノアは大規模なセキュリティ侵害を受けた別の金融機関の顧客になりました。ノアは、個人情報漏洩した何百万人もの顧客の1人でした。彼は、自分が個人情報盗難の被害者になったのではないかと、またそれが自分の信用に悪影響を与えたのではないかと考えています。

ノアは、これらの困難をすぐに乗り越え、優れた信用を築き、完璧な仕事を見つけられるようになることを望んでいます。

このシナリオに基づいて、アーニーズ・エンポリウムに申し込んだ結果生じたノアの信用報告書に関する不安を和らげる法律はどれでしょうか？

- A. グラム・リーチ・ブライリー法 (GLBA) に基づくプライバシー規則。
- B. グラム・リーチ・ブライリー法 (GLBA) に基づく保障措置規則。
- C. 公正かつ正確な信用取引法 (FACTA) に基づく処分規則。
- D. 公正かつ正確な信用取引法 (FACTA) に基づくレッドフラッグルール。

Answer: [\(解答を表示する\)](#)

商務省 (DOC) は、民間セクター向けの自主的な行動規範、基準、ベストプラクティスの開発と採用を推進し、EU-US プライバシーシールドや APEC 越境プライバシールールなどのメカニズムを通じて国境を越えたデータ転送を促進することで、プライバシーポリシーに役割を果たしています。ただし、DOC にはプライバシー法を施行したり、プライバシー侵害に対する制裁を課したりする規制権限はありません。リストされている他の機関は、それぞれの領域内でプライバシーの問題に関してある程度の規制権限を持っています。たとえば、通貨監督庁 (OCC) は国立銀行と連邦貯蓄協会を監督し、これらの機関に対して GLBA プライバシーおよびセキュリティルールを施行しています。連邦通信委員会 (FCC) は州間および国際通信を規制し、電気通信事業者、ブロードバンドプロバイダー、およびボイスオーバーインターネットプロトコル (VoIP) サービスに対してプライバシーおよびセキュリティルールを施行しています。運輸省 (DOT) は運輸部門を監督し、航空運輸保安法 (ATSA) に基づいて航空会社、旅行代理店、その他の対象事業体に対するプライバシーとセキュリティのルールを施行しています。参考資料:

* IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第1章:

U.S. プライバシー環境、セクション 1.3: プライバシーに関与する連邦機関、p. 18-19

* IAPP CIPP/US Body of Knowledge、ドメイン I: 米国のプライバシー環境の概要、目標 IB: プライバシーに関係する主要な連邦機関を特定する、サブ目標 IB4: 商務省の役割を特定する、p. 7

* IAPP CIPP/US 試験ブループリント、ドメイン I: 米国のプライバシー環境の概要、目標 I。B: プライバシーに関する役割を持つ主要な連邦機関を特定する、サブ目標 IB4: 商務省の役割を特定する、p. 3

最新問題: 49

シナリオ

次の質問に回答するには、以下を使用してください。

ラリーは、サンライズリンクスでのテレマーケティングの職務、特に上司のエヴァンにますます不満を募らせている。先週、エヴァンが州の Do Not Call リストとそこに載っている人々をあざ笑っているのを耳にした。迷惑をかけたくないと本気で思っているなら、全国 DNC リストに載っているはずだ。それが私たちが従わなければならない唯一のリストだ。サンライズリンクスでは、電話しないでほしいと言われるまで電話をかけ続ける」。奇妙なことに、エヴァンはテレマーケティング担当者に、受信者が 別の機会に」電話してほしいと頼んだ場合の記録を残すよう要求している。ラリーにとって、これは彼らがまったく電話を受けたくないという明らかな兆候だ。エヴァンはそうは考えていない。

ラリーは、エヴァンの傲慢さが従業員への接し方にも影響していると考えています。米国憲法は米国の労働者を保護しており、ラリーはサンライズリンクスの従業員の権利が定期的に侵害されていると考えています。最初、エヴァンはソーシャルメディアで従業員と交流するなど、友好的に見えました。しかし、エヴァンの政治的な投稿を見て、昇進を申し出られるのは同じような立場の従業員だけであることがラリーには明らかになりました。

さらに、ラリーは時々、私的使用の品が入った小包を職場に郵送してもらっています。名前がはっきり記されているにもかかわらず、すでに開封された状態で届いたことが何度かありました。ラリーは、サンライズリンクスでは私的郵便物の開封は一般的であり、エヴァンのリーダーシップの下では憲法修正第 4 条の権利が踏みにじられていると考えています。

ラリーは同僚のセイディーに関する会話を耳にして落胆したこともある。テレマーケティングの電話は品質保証のために定期的に録音されており、セイディーは仕事中は常にプロフェッショナルだが、私的な会話には性的な発言が含まれることがある。ラリーはエヴァンがこれについても笑っているのを聞いたことがある。彼が同僚にこのことを話すと、彼の懸念は肩をすくめるだけで済んだ。同僚は、従業員は入社時に監視されることに同意していると思っていた。個人のデバイスには手を付けていないが、電話、メール、閲覧履歴はすべて監視対象となっている。実際、ラリーは、外部の会社による覆面調査で不正行為の証拠が見つかり、従業員が解雇された事例を1件知っている。その従業員は会社から盗んだのかもしれないが、エヴァンは何かおかしいと最初に疑った時点で当局に連絡すればよかったのだ。

ラリーは行動を起こしたいと思っていますが、どのように進めればよいかわかりません。どの行為がエヴァンの潜入捜査を許可するのでしょうか？

- A. 内部告発者保護法
- B. 保存通信法 (SCA)
- C. 全国労働関係法 (NLRA)
- D. 公正かつ正確な信用取引法 (FACTA)

Answer: [\(解答を表示する\)](#)

保存通信法 (SCA) は、電子メール プロバイダー、クラウドストレージ プロバイダー、ソーシャルメディア プラットフォームなどのサードパーティ サービス プロバイダーによって保存される電子通信のプライバシーを規制する連邦法です。SCA は、法律で許可されている場合、またはユーザーやサービス プロバイダーの同意がある場合を除き、そのような通信への不正アクセスや開示を禁止しています。また、SCA は、法執行目的、サービス プロバイ

ダーの権利や財産の保護、加入者や顧客の同意など、特定の種類のアクセスや開示に対しては例外を設けています。

SCA の例外の 1 つは、サービス プロバイダーが保存された通信へのアクセスまたは開示に同意する場合です。つまり、サードパーティのサービス プロバイダーが調査または情報要求に協力することに同意した場合、そのアクセスまたは開示は SCA の下で合法です。同意は、状況とプロバイダーの利用規約に応じて、明示的または暗黙的になります。たとえば、サービス プロバイダーが正当な目的でユーザー情報をサードパーティに開示することを許可するポリシーを持っている場合、プロバイダーは保存された通信へのアクセスまたは開示に暗黙的に同意しています。ただし、サービス プロバイダーがそのような開示を禁止するポリシーを持っている場合、プロバイダーは保存された通信へのアクセスまたは開示に同意していません。

このシナリオでは、エヴァンの潜入捜査は、不正行為の疑いのある従業員の電子通信を保存しているサードパーティのサービスプロバイダーの同意を得ていれば、SCA によって承認されていた可能性があります。たとえば、従業員が会社のメールアカウントやクラウドストレージサービスを使用していて、そのサービスプロバイダーがユーザー情報を雇用主や法執行機関に開示することを許可するポリシーを持っていた場合は、エヴァンはサービスプロバイダーの同意を得て、保存されている通信にアクセスしたり開示したりできた可能性があります。しかし、従業員が個人のメールアカウントやクラウドストレージサービスを使用していて、ユーザーのプライバシーを保護し、そのような開示を禁止するポリシーを持っていた場合は、エヴァンはサービスプロバイダーの同意なしに保存されている通信にアクセスしたり開示したりすることで、SCA に違反した可能性があります。

参照文献: [蓄積通信法]、18 USC §§ 2701-2712 : [IAPP CIPP/US 学習ガイド]、第 8 章、セクション 8.2.2。: [蓄積通信法: 現代の問題に対する古い法律]、pp. 10-11.

最新問題: 50

シナリオ

次の質問に回答するには、以下を使用してください。

シェリルは、Fitness Coach, Inc. の唯一の所有者です。同社は、クラス、個人指導、大規模な屋内ジムへのアクセスを通じて、個人のフィットネス目標の実現を支援する中規模企業です。彼女は 10 年間この会社を経営しており、常に最高レベルのサービスを維持しながら顧客のプライバシーを保護することに配慮してきました。彼女は、顧客と長期にわたる関係を築いてきたことを誇りに思っています。

シェリルとスタッフはプライバシー保護を最優先にしようと努めてきましたが、会社には正式なプライバシーポリシーがありませんでした。そこでシェリルはプライバシーの専門家であるジャニスを雇い、ポリシーの作成を手伝ってもらいました。

最初の評価の後、ジャニスは新しいポリシーの最初のものを作成しました。シェリルは草案を読み、このポリシーが会社全体にもたらす多くの変更を懸念しました。たとえば、草案では、パーソナルトレーナーとのセッションなどのサービスに対して顧客の個人情報を支払っ

た後、1年間のみ保持できると規定されています。また、顧客の書面による同意なしに顧客情報を第三者と共有しないことも約束しています。これらの規則の文言はシェリルを心配させます。なぜなら、保存された個人情報、顧客が長い間訪問していなくても、会社が顧客にサービスを提供するのに役立つことが多いからです。さらに、契約ベースでクラスを教えるエアロビクスのインストラクターなど、重要なサービスを提供するサードパーティもいます。顧客ファイルにアクセスし、生徒のフィットネスレベルを理解することは、インストラクターがクラスを編成するのに役立ちます。

ジャニス はシェリルの懸念を理解し、すでにいくつかの修正案を練っていました。顧客データは保持できるが、機密性のレベルに応じて分類する必要があることを指摘して、シェリルを安心させようとしていました。しかし、シェリルは懐疑的でした。データを分類し、タイプごとに異なる取り扱いをすると、会社の日常業務に不必要な困難が生じるように思われました。シェリルは、必要に応じてすべての従業員がアクセスできる、1つのシンプルなデータストレージおよびアクセスシステムを望んでいます。

プライバシーポリシーはまだ草案に過ぎませんでした。彼女は社内に変更が必要になるだろうと感じ始めていました。彼女はジャニスに、数か月かけて1部門ずつ新しいポリシーを徐々に導入する方が安心できるだろうと伝えました。また、新しいポリシーの適用可能な部分を各部門にリストしたドキュメントを作成するという階層化アプローチにも興味がありました。

このシナリオに基づいて、ジャニスが会社のニーズをよりよく満たすために役立つと思われるのは次のうちどれですか。

- A. 新しいポリシーを実施するためのより包括的な計画を作成する
- B. 企業の情報目標を理解するためにより多くの時間を費やす
- C. 新しいポリシーを実施する際の透明性の重要性を説明する
- D. 会社の従業員研修プログラムの経済的負担を軽減する

Answer: B (メッセージを残す)

Wiley の学習ガイドによると、プライバシーポリシーを作成する手順の1つは、プライバシー評価を実施することです。この評価には、組織の情報目標とニーズ、およびデータ収集と使用の慣行に適用される法律と規制の要件の特定が含まれます³。会社の情報目標を理解するためにもっと時間を費やすことで、Janice は、関連するプライバシー法と基準に準拠しながら、会社のビジネスモデルと顧客の期待に合わせてプライバシーポリシーをカスタマイズできたはずでした。また、これにより、Janice は、ポリシーが会社の運営と顧客関係に与える影響についての Cheryl の懸念に対処し、プライバシー保護とサービス提供のバランスをとるソリューションを提案することができました。

参考文献:

1: <https://iapp.org/certify/cippus/>

2: <https://iapp.org/certify/get-certified/cippus/>

3: <https://www.wiley.com/en-be>

/IAPP+CIPP+US+認定+情報+プライバシー+プロフェッショナル+学習ガイド-
p-9781119755517

4: <https://www.techtarget.com/searchsecurity/quiz/10-CIPP-US-practice-questions-to-test-your-privacy-knowledge>

5: <https://www.study4exam.com/iapp/free-cipp-us-questions>

<https://www.passitcertify.com/iapp/cipp-us-questions.html>

最新問題: 51

法執行機関は、ACME 通信会社に対し、テロ攻撃を計画した疑いのある人物のテキストメッセージ記録へのアクセスを求める召喚状を発行しました。同社は以前、テキストメッセージ記録を暗号化し、容疑者だけがこのデータにアクセスできるようにしていました。

ACME は、法執行機関による情報へのアクセスを防ぐサービスを設計することで、どのような法律に違反したのでしょうか？

- A. SCA
- B. ECPA
- C. パス
- D. 米国自由法

Answer: C (メッセージを残す)

ACME が法執行機関による情報へのアクセスを防ぐサービスを設計することで違反した法律は、法執行のための通信支援法 (CALEA)¹ です。CALEA は連邦法であり、通信キャリアと通信機器メーカーに、通信傍受の法的要請に応じるために必要な監視機能を備えるように機器、施設、サービスを設計することを求めています²。CALEA はテキストメッセージを含むすべての商用メッセージに適用され、法執行機関にサービス プロバイダーからそのような通信の記録を召喚する権限を与えています³。ACME は、容疑者だけがこのデータにアクセスできるようにテキストメッセージの記録を暗号化することで、法執行目的での通信の傍受に協力するという CALEA の義務に違反しました。参考文献: 1: 法執行のための通信支援法 -

Wikipedia²: ホーム | CALEA | 法執行機関認定委員会、Inc.³: 法執行機関向け通信支援法:

IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第 6 章: 法執行機関と国家安全保障アクセス、p. 177

最新問題: 52

USA FREEDOM法ではどのような行為が認められていないのでしょうか？

- A. 政府が徘徊者をターゲットにすることを可能にする緊急例外
- B. テロへの物質的支援に対する最高刑の引き上げ
- C. 移動盗聴の有効期限の延長
- D. 電話データとインターネットメタデータの一括収集

Answer: (解答を表示する)

説明/参照: <https://www.rand.org/blog/2015/05/the-usa-freedom-act-the-definition-of-a-compromise.html>

最新問題: 53

公正かつ正確な信用取引法 (FACTA) に基づく「レッドフラッグルール」は、送金サービスを利用する食料品店のオーナーとどのような関係がありますか？

- A. 信用記録を保護するために最新の技術の使用を義務付けている
- B. 所有者は個人情報盗難警告システムを実装する必要があります
- C. 小規模金融機関の場合、通常は適用されない
- D. 所有者は債権者ではないため適用されません

Answer: D (メッセージを残す)

レッドフラッグルールは、金融機関および債権者に対し、対象口座の開設または既存の対象口座に関連する個人情報の盗難を検出、防止、および軽減するように設計された書面による個人情報盗難防止プログラムの実施を要求する規制です¹。債権者とは、定期的に信用を延長、更新、または継続する人、信用の延長、更新、または継続を定期的に手配する人、または信用の延長、更新、または継続の決定に参加する元の債権者の譲受人です²。対象口座とは、金融機関または債権者が主に個人、家族、または世帯の目的で提供または維持する口座で、複数の支払いまたは取引を伴うか、または許可するように設計されている口座で、クレジットカード口座、住宅ローン、自動車ローン、証拠金口座、携帯電話口座、公共料金口座、当座預金口座、または普通預金口座などです²。送金サービスは、顧客が電子的に送金または受け取りを行えるサービスです³。送金サービスを利用する食料品店のオーナーは、顧客への信用を定期的に延長、更新、継続していないため、債権者ではありません。したがって、送金サービスを利用する食料品店のオーナーにはレッドフラッグルールは適用されません。参考資料:

* 1: FTC、レッドフラッグルール、<https://www.ftc.gov/business-guidance/privacy-security/red-flags-rule>

* 2: FTC、「レッドフラッグルールによる個人情報盗難対策 :ビジネス向けハウツーガイド」
<https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide->

* 3: アレッサ、電信送金の危険信号: マネーロンダリングと詐欺のリスクを理解する、
<https://alessa.com/webinars/wire-transfer-red-flags-and-fraud-risks/>

最新問題: 54

マーケティング担当者にワイヤレス ドメイン レジストリの使用を義務付ける主な目的は何ですか？

- A. 現在の無線ドメイン名のリストにアクセスする
- B. モバイルデバイスへの不正なメールを防ぐため
- C. モバイルデバイスにメールを送信するための承認を取得する
- D. メールが実際のワイヤレス加入者に確実に送信されるようにするため

Answer: B (メッセージを残す)

ワイヤレス ドメイン レジストリは、携帯電話やポケベルなどのワイヤレス デバイスに電子メッセージを送信するために使用されるドメイン名のリストです。レジストリの目的は、そのようなメッセージを送信する人のドメイン名を特定することにより、ワイヤレス コンシューマーを不要な商用電子メール メッセージから保護することです。マーケティング担当者は、ワイヤレス デバイスに迷惑メールを送信しないようにレジストリを使用する必要があります。

ります。迷惑メールは受信者にコストや不便をもたらす可能性があります。受信者の明示的な事前の許可なしにこのようなメールを送信することは、2003年のCAN-SPAM法に違反します。参照: <https://www.fcc.gov/cgb/policy/>

ドメイン名入力

<https://www.prnewswire.com/in/news-releases/the-wireless-registry-launches-worlds-first-global-registry-for-wireless-names-240222521.html>

最新問題: 55

職場を離れた従業員に対する雇用主のプライバシー関連の責任を最もよく表しているのはどれですか？

- A. 雇用主は、差別などの会社に対する請求を裏付けるために必要なコンピュータシステムと会社のデータへの元従業員のアクセスを維持する責任があります。
- B. 雇用主は、雇用主と元従業員の両方に対するプライバシーのリスクを最小限に抑えるために、すべての機密雇用記録を永久に削除または消去する責任があります。
- C. 雇用主と従業員の関係は主に契約上のものであると考えられるため、雇用主はプライバシー関連の責任が終了したとみなすことができます。
- D. 雇用主は、正当な業務目的で保持される機密性の高い雇用記録のセキュリティとプライバシーを維持する責任があります。

Answer: [\(解答を表示する\)](#)

雇用主は、現在および過去の従業員、ならびに応募者の個人情報に不正アクセス、使用、または開示から保護する義務を負っています。この義務は、公正信用報告法 (FCRA)、医療保険の携行性と責任に関する法律 (HIPAA)、カリフォルニア州消費者プライバシー法 (CCPA) などの連邦法または州法、または秘密保持契約やプライバシーポリシーなどの契約上の義務から生じる場合があります。雇用主は、法的要件の遵守、訴訟の防御、監査の実施などの正当なビジネス目的で、業績評価、懲戒処分、医療記録、または経歴調査などの機密性の高い雇用記録を保持する場合があります。ただし、雇用主は、これらの記録が安全に保管され、許可された担当者のみがアクセスでき、不要になった場合は適切に廃棄されるようにする必要があります。参考文献: IAPP CIPP/US 学習ガイド、第 4 章、セクション

4.1.1、IAPP CIPP/US 知識体系、ドメイン IV、目標 B

最新問題: 56

Global Manufacturing Co の人事部は最近、新しいソフトウェア ツールを購入しました。このツールは、メールをスキャンして候補者の発言や候補者について言われている内容を確認し、幹部候補を評価するのに役立ちます。これにより、人事部は自動化された「360 度評価」を行えるようになり、候補者の考え方や行動、同僚や直属の部下が候補者について何を言っているか、候補者同士のやり取りがどの程度うまくいっているかを知ることができます。この新しいソフトウェアを導入する際に人事部門が行う最も重要なステップは何ですか？

- A. ソフトウェアが保護されたグループに対して意図せず差別を行わないようにします。

B. 従業員が組織のシステムでこのソフトウェアを実行して電子メールシステムをスキャンしている限り、従業員にはプライバシーの権利がないことを説明するプライバシー通知がソフトウェアに含まれていることを確認します。

C. 従業員が従業員ハンドブックを読んで署名したことを確認します。従業員ハンドブックには、EEOC によって施行される保護対象グループや法律に関係なく、組織のシステムを使用している限り、プライバシーの権利がないことが記載されています。

D. 従業員に、電子メールがソフトウェアによってスキャンされ、自動プロフィールが作成されることを通知します。

Answer: D (メッセージを残す)

この新しいソフトウェアを導入する際に人事部門が行うべき最も重要なステップは、従業員に、ソフトウェアによって電子メールがスキャンされ、自動プロフィールが作成されることを通知することです。これは、ソフトウェアが従業員の個人情報を収集して使用するため、従業員のプライバシー権と期待に影響を及ぼす可能性があるためです。通知を行うことで、人事部門は従業員にソフトウェアの目的、範囲、結果、およびデータに関する従業員の選択肢と権利について知らせることができます。通知は、プライバシー管理の重要な原則である透明性と説明責任の重要な要素でもあります。通知を行うことで、人事部門は、電子通信プライバシー法 (ECPA)、保存通信法 (SCA)、公正信用報告法 (FCRA)、州のプライバシー法など、ソフトウェアに適用される可能性のあるさまざまなプライバシー法や規制に準拠できます。通知は、プライバシー侵害、契約違反、従業員の権利侵害の申し立てなど、ソフトウェアから生じる可能性のある潜在的な法的リスクや責任を回避するのにも役立ちます。参考資料:

* Peter P. Swire, DeBrae Kennedy-Mayo 著 『国民間部門のプライバシー』第 3 版、第 4 章、セクション 4.2.1、97-98 ページ。

* Peter P. Swire, DeBrae Kennedy-Mayo 著 『国民間部門のプライバシー』第 3 版、第 5 章、セクション 5.2.1、125-126 ページ。

* Peter P. Swire, DeBrae Kennedy-Mayo 著 『国民間部門のプライバシー』第 3 版、第 6 章、セクション 6.2.1、153-154 ページ。

* Mike Chapple および Joe Shelley 著 『APP CIPP/US 認定情報プライバシー専門家学習ガイド』、第 4 章、セクション 4.1、113 ~ 114 ページ。

最新問題: 57

どのようなプライバシー概念によって、消費者は自分の信用報告書の誤りを閲覧し、修正する権利を与えられるのでしょうか？

A. アクセス。

B. 注意してください。

C. アクション。

D. 選択。

Answer: A (メッセージを残す)

アクセスとは、組織が保有する個人情報を閲覧する能力です。これは、情報の更新や修正を許可することで補完される場合があります。米国の法律では、信用報告書などの実質的な意思決定に情報が使用される場合、アクセスと修正が認められることが多いです。」

最新問題: 58

企業のプライバシー プログラムを開発する際に、プライバシー専門家が組織に役立つガイダンスを開発するのに最も役立つ関係は次のどれですか。

- A. さまざまな業界の専門知識と最先端のプラクティスを共有できるプライバシー専門家コミュニティ内の個人との関係。
- B. 組織のプログラム全体で主にデータが収集され使用されるクライアント、ベンダー、顧客との関係。
- C. 企業のプライバシー プログラムの承認、実装、定期的なレビューを担当する会社のリーダーとの関係。
- D. 会社の部門間および組織階層内のさまざまなレベルの個人との関係。

Answer: D (メッセージを残す)

企業のプライバシー プログラムを開発する場合、プライバシー プロフェッショナルは、組織のビジネス目標、プロセス、リスク、およびプライバシーに関する法律と規制の要件とベストプラクティスを理解する必要があります。これを実現するには、プライバシー プロフェッショナルは、IT、マーケティング、人事、法務、コンプライアンス、セキュリティ、上級管理職など、組織の階層内のさまざまなレベルの企業部門の個人との関係を確立し、維持する必要があります。これらの関係は、プライバシー プロフェッショナルが関連情報を収集し、プライバシーの問題とギャップを特定し、プライバシー ポリシーと手順を伝え、トレーニングと意識向上を提供し、コンプライアンスを監視し、競合を解決するのに役立ちます。

記載されている他の関係も重要ですが、企業のプライバシー プログラムを開発する上で内部関係ほど重要ではありません。参考資料:

* IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第 5 章: プライバシー プログラムの開発、セクション 5.1: プライバシー プログラム フレームワーク、p. 145-146

* IAPP CIPP/US 知識体系、ドメイン V: プライバシー プログラムの開発、目標 VA: プライバシー プログラム フレームワークのコンポーネントを特定する、サブ目標 VA1: 組織内の個人の役割と責任を特定する、p. 23

* IAPP CIPP/US 試験ブループリント、ドメイン V: プライバシー プログラムの開発、目標 VA: プライバシー プログラム フレームワークのコンポーネントを特定する、サブ目標 VA1: 組織内の個人の役割と責任を特定する、p. 7

最新問題: 59

ある企業の従業員向けウェルネス ポータルでは、ユーザーのモバイル デバイスを介して運動活動を追跡するアプリを提供しています。アプリの使用時に、ユーザーにデータのプライバシー権と特権を最も効果的に知らせる設計手法は次のどれですか。

- A. ウェルネス プログラムの登録プロセス中に、ユーザーにプライバシー ポリシーを提示します。
- B. 主要なデータ入力ポイントでデータの収集と使用に関する情報を提供します。
- C. 各画面の下部に、ウェルネス プログラムのプライバシー ポリシーへのリンクを提供します。
- D. 明確かつ簡潔で理解しやすい言葉で書かれたプライバシー ポリシーを公開します。

Answer: A (メッセージを残す)

最新問題: 60

次の情報のうち、組織が法執行機関に開示する必要のない情報はどれですか？

- A. 食品医薬品化粧品法に基づく投薬ミスに関する情報
- B. HIPAA プライバシー規則に基づく個人健康情報
- C. 1970 年銀行秘密法に基づくマネーロンダリング情報
- D. OSHA の要件に基づく職場での傷害に関する情報

Answer: (解答を表示する)

最新問題: 61

連邦取引委員会がBJ's Wholesale Clubに対して行った措置の特徴は何だったのか？
2005年ですか？

- A. 第三者による監査をポリシー違反に対する罰則としました。
- B. それは欺瞞ではなく公平さの問題に基づいていました。
- C. これは、米国と EU 間のセーフ ハーバーに関する初の実質的な施行でした。
- D. ポリシーの改訂後には必ずユーザーの同意が必須になりました。

Answer: B (メッセージを残す)

連邦取引委員会 (FTC) は、米国における消費者プライバシーおよびデータ セキュリティ法を執行する主要な連邦機関です。FTC は、FTC 法第 5 条に基づき、商取引に影響を及ぼす不公正または欺瞞的な行為や慣行に関与する企業に対して執行措置を講じる権限を有しています。

不公正な行為または慣行とは、消費者が合理的に回避できず、消費者または競争に対する相殺利益によって上回られない、消費者に重大な損害を引き起こす、または引き起こす可能性のある行為または慣行を指します。欺瞞的な行為または慣行とは、状況下で合理的に行動する消費者を誤解させる可能性のある重要な表示、省略、または慣行を伴う行為または慣行を指します。

2005 年の BJ's Wholesale Club に対する FTC の措置は、欺瞞ではなく公平性の問題に基づいていたという点で特異なものでした。FTC は、倉庫型店舗とガソリンスタンドを運営する小売業者である BJ's Wholesale Club が、クレジットカードやデビットカードの磁気ストライプから収集した名前、カード番号、有効期限などの顧客の機密情報に対して適切なセキュリティを提供できなかったと主張しました。FTC は、この情報が権限のない人物によって使用され、数百万ドルの不正購入が行われたと主張しました。FTC は、BJ's Wholesale Club がデータ セキュリティ慣行に関して虚偽または誤解を招くような陳述や省略を行ったとは主張

していませんが、適切なセキュリティ対策を講じなかったことは、FTC 法第 5 条に違反する不公正な慣行であると主張しています。FTC は、BJ's Wholesale Club のセキュリティが不十分だったために、消費者が合理的に回避できず、消費者や競争への利益によって上回られることのない重大な損害が消費者に生じたか、生じる可能性があったと主張しました。

FTC による BJ's Wholesale Club に対する措置は、FTC が不公平行為権限を使用してデータセキュリティの問題に対処した最初のケースの 1 つであり、消費者データを保護できない企業に対する今後の執行措置の先例となりました。和解により、BJ's Wholesale Club は包括的な情報セキュリティ プログラムを導入し、20 年間にわたり 2 年ごとに独立した第三者セキュリティ専門家による監査を受けることが義務付けられました。参考資料:

* FTC 苦情、第1-23段落

* 同意命令を含むFTC協定、第1～9項

* パブリックコメントを支援するための同意命令案の FTC 分析、1 ～ 3 ページ

* [IAPP CIPP/US 学習ガイド]、69-70ページ

有効な **CIPP-US** 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集！ GoShiken.com が最新の **CIPP-US** 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (228**30%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 62

次の組織のうち、顧客に毎年プライバシー通知を提供する必要があるのはどれですか？

- A. キング郡貯蓄貸付組合。
- B. フォーウィンズ部族大学。
- C. ブリッジーシティ住宅委員会。
- D. ゴールデン ギャベル オークションハウス。

Answer: ([解答を表示する](#))

最新問題: 63

公正信用報告法 (FCRA) に基づき、信用履歴に基づいて雇用を拒否された人は何を受ける必要がありますか？

- A. 消費者金融保護局 (CFPB) からの権利のリスト。
- B. 雇用主に再応募する機会。
- C. 複数の消費者信用情報機関 (CRA) からの情報。
- D. 雇用主からの迅速な通知。

Answer: D ([メッセージを残す](#))

最新問題: 64

米国におけるパンデミック接触追跡アプリの規制状況を最も正確に説明しているのは次のどれですか？

- A. 接触追跡は、医療保険の携行性と責任に関する法律 (HIPAA) のみの対象となります。
- B. 接触者追跡は米国疾病予防管理センター (CDC) によって規制されています。
- C. 接触追跡は連邦および州のプライバシー法の寄せ集めの対象となる
- D. 米国では接触追跡は規制されていません。

Answer: ([解答を表示する](#))

米国では、パンデミック接触追跡アプリは、単一の包括的な枠組みではなく、連邦および州のプライバシー法の寄せ集めに基づいて規制されている。接触追跡の取り組みには、位置情報や健康情報などの機密データの収集と処理が含まれることが多く、管轄区域やデータの種類に応じて異なる法的制度の対象となる可能性がある。

接触追跡アプリに影響を与える主な規制:

* 州のプライバシー法:

* カリフォルニア州 カリフォルニア州消費者プライバシー法 - CCPA)などの州では、特に個人データが収集または共有される場合に、接触追跡アプリに適用される可能性があるプライバシー法が定められています。

* 州レベルの健康プライバシー法によって、健康関連データの収集方法と使用方法も規定される場合があります。

* HIPAA:

* HIPAA (医療保険の携行性と責任に関する法律) は、アプリが対象事業体 (医療提供者や健康保険など) によって、またはその代理で使用される場合にのみ適用されます。アプリが HIPAA 対象事業体と関係のない民間企業によって運営されている場合、HIPAA は適用されない可能性があります。

* 連邦政府のガイダンス:

* 連邦取引委員会 (FTC) は、不公正または欺瞞的な行為を禁止する FTC 法第 5 条に基づいて一般的なプライバシー保護を実施しています。

* FTC は、健康関連アプリのプライバシーに関する考慮事項に関するガイダンスも発行しています。

* その他の連邦法およびセクター固有の法律:

* アプリが健康関連のデータを収集する場合、アメリカ障害者法 (ADA) などの法律や業界固有の規則に基づく義務が発生する可能性もあります。

オプションの説明:

* A. 接触追跡は、医療保険の携行性と責任に関する法律 (HIPAA) のみの対象です。これは誤りです。HIPAA は対象となる事業体とそのビジネス関連者にのみ適用され、すべての接触追跡アプリや取り組みに広く適用されるわけではありません。

* B. 接触者追跡は米国疾病予防管理センター (CDC) によって規制されています。

これは誤りです。CDC は公衆衛生に関するガイダンスと推奨事項を提供していますが、接触追跡アプリに対する規制権限はありません。

* C. 接触追跡は連邦および州のプライバシー法の寄せ集めの対象です。これは正解です。米国の接触追跡アプリは、さまざまな連邦法、州法、および業界固有の法律によって規制されており、不完全な規制枠組みを形成している。

* D. 接触者追跡は米国では規制されていない: これは誤りです。接触者追跡には単一の規制枠組みはありませんが、この行為は複数の連邦法と州法の対象となります。

CIPP/US 資料からの参照:

* IAPP CIPP/US 認定テキスト: 接触追跡アプリを含む健康関連テクノロジーへの HIPAA、州のプライバシー法、連邦規制の適用について説明します。

* 健康アプリに関する FTC ガイダンス: 健康関連データを扱うアプリ開発者向けのプライバシーに関する考慮事項について詳しく説明します。

最新問題: 65

「電子情報開示」の規則は主に次のどれを防止しますか?

- A. ビジネス慣行と技術的安全対策の矛盾
- B. 不適切なデータ保持方法による情報の損失
- C. 従業員が個人所有のデバイスを仕事に利用する慣行
- D. 組織のデータ保持プログラムの違反

Answer: ([解答を表示する](#))

電子情報開示とは、当事者が電子的に保存された情報 (ESI) を共有、確認、収集し、法的事項の証拠として使用するプロセスです¹。電子情報開示の規則は、訴訟のニーズとテクノロジーの現実のバランスをとる方法で ESI を保存、収集、確認、および作成するための標準と手順を確立するため、主にビジネス慣行とテクノロジーの保護手段の間の矛盾を防ぎます²。たとえば、連邦民事訴訟規則 (FRCP) は、電子情報開示の範囲、タイミング、形式、方法、および電子情報開示の義務に従わなかった場合の制裁に関するガイダンスを提供します³。この規則は、電子情報開示の問題を効率的かつ効果的に解決するために、当事者と裁判所間の協力とコミュニケーションも奨励しています⁴。電子情報開示の規則に従うことで、当事者は、互換性のない、または一貫性のないビジネス慣行とテクノロジー慣行から生じる可能性のある紛争、遅延、およびコストを回避できます。

その他のオプションは、eDiscovery 規則の主な目的ではありませんが、eDiscovery 規則と関連したり、eDiscovery 規則の影響を受ける可能性があります。eDiscovery 規則は、訴訟が合理的に予想される場合に、関連する ESI を保存する義務を課していますが、不適切なデータ保持慣行による情報の損失を直接防止するものではありません⁵。eDiscovery 規則は、従業員が個人用デバイスを仕事に使用する慣行を直接防止するものではありません⁶。ただし、当事者に、個人用デバイスを含む、開示の対象となる可能性のある ESI のソースを特定して開示することを要求しています⁶。eDiscovery 規則は、組織のデータ保持プログラムの違反を直接防止するものではありません⁷。ただし、当事者に、ESI を合理的に使用可能な形式で作成し、特権情報または機密情報を保護することを要求しています⁷。

参考文献: 1: 「E-Discovery について知っておくべきことすべて」、The National Law

Review。2: 「E-Discovery: E-Discovery の基本ガイド - Exterro」、Exterro.com。3: 連邦裁判所

および政府機関の E-Discovery のルールとガイドライン」、Crowell & Moring LLP。4: FRCP ルール 1」、コーネル大学ロースクール。5: FRCP ルール 37」、コーネル大学ロースクール。6: FRCP ルール 26」、コーネル大学ロースクール。7: FRCP ルール 34」、コーネル大学ロースクール。

最新問題: 66

公民権法第 7 条では、雇用主が求職者に質問することを禁止しているのは次のどれですか。

- A. 国籍に関する質問
- B. 妊娠予定に関する質問
- C. 年齢に関する質問
- D. 障害に関する質問

Answer: ([解答を表示する](#))

最新問題: 67

プライバシーに対する欧州のアプローチを支持する人の中に、プライバシー慣行の自主規制に懐疑的な人がいる主な理由は何ですか？

- A. 業界はルールの作成と施行に十分厳格ではない可能性がある
- B. 新規事業主は規制を理解していない可能性がある
- C. 技術とセキュリティの向上に多額の資金を投入する必要があるかもしれない
- D. プライバシーのために人権が無視される可能性がある

Answer: ([解答を表示する](#))

最新問題: 68

カリフォルニア州に拠点を置く Privacy Is Hiring Inc. は、大手企業の役職にプライバシー専門家を派遣することに重点を置いたオンライン専門人材紹介会社です。求職者は、自分の経験や資格を記したオンラインプロフィールを作成し、クレジットカードで月額 19.99 ドルを支払うことで、自分のプロフィールを潜在的な雇用主に宣伝することができます。Privacy Is Hiring Inc. は、すべての顧客データを暗号化してサーバー上に保管しています。

どのような状況で、Privacy Is Hiring Inc. はデータ侵害が発生した場合に影響を受ける個人に通知する必要がありますか？

- A. 法執行機関が捜査を完了し、Privacy Is Hiring Inc. がクライアントおよび該当する規制当局に通知を提供することを許可した場合。
- B. 盗まれた情報の中に求職者のクレジットカード情報や暗号化キーが含まれていた場合。
- C. Privacy Is Hiring Inc. が、データ漏洩によって求職者が被害を受けると合理的に判断した場合。
- D. 盗まれた個人情報に個人の名前やクレジットカードの暗証番号が含まれていた場合。

Answer: ([解答を表示する](#))

カリフォルニア州消費者プライバシー法 (CCPA) に基づき、カリフォルニア州の居住者の個人情報を収集する企業は、合理的なセキュリティ手順と慣行を実施および維持する義務に違

反した結果、個人情報不正アクセスされ、流出、盗難、または開示された場合、データ侵害について通知する必要があります。ただし、CCPA では、暗号化キーまたはセキュリティ認証情報も侵害されない限り、暗号化または編集された個人情報は個人情報の定義から除外されます。したがって、Privacy Is Hiring Inc. は、クレジットカード情報とともに暗号化キーも盗まれた場合にのみ、影響を受けた個人に通知する必要があります。そうしないと、暗号化が無効になり、個人情報が不正アクセスにさらされることになります。その他のオプションは、CCPA の通知要件とは関係ありませんが、他の法律やベスト プラクティスには関係する可能性があります。参考文献: CCPA (セクション 1798.150)、IAPP CIPP/US 学習ガイド (p. 63-64)

最新問題: 69

サラはカリフォルニア州サンフランシスコに住んでいます

a. 迷惑な商業メールが急増していることから、サラさんは、5,000 万人以上のユーザーを抱える大手ソーシャル メディア プラットフォームが自分の個人情報を大量に収集していると考えています。このプラットフォームを運営する会社は、ニューヨークとフランスに拠点を置いています。

なぜサラはソーシャル メディア プラットフォームに対して、彼女について収集された個人情報を削除するよう要求する権利があるのでしょうか？

- A. カリフォルニア州消費者プライバシー法により、サラは自分の個人情報の削除を要求する権利を有します。
- B. FTC 法第 5 条に基づき、連邦取引委員会は、個人の個人情報の削除要求を拒否することは不公正な行為に当たると判断しました。
- C. ヨーロッパに拠点を置く企業は、データ主体の削除要求への対応を含め、世界的に一般データ保護規則に準拠する必要があります。
- D. ニューヨーク州の「ハッキングを阻止し、電子データ セキュリティを強化する」(SHIELD) 法では、ニューヨーク州の管轄下にある企業は、要求に応じて顧客の個人情報を削除することが義務付けられています。

Answer: A (メッセージを残す)

最新問題: 70

Mega Corp. は、カリフォルニア州、バージニア州、コロラド州に従業員を擁する米国企業です。Mega Corp. は、人事データに関して次のどれに準拠する必要がありますか？

- A. カリフォルニア州プライバシー権利法およびバージニア州消費者データ保護法。
- B. カリフォルニア州プライバシー権法、バージニア州消費者データ保護法、コロラド州プライバシー法。
- C. カリフォルニア州プライバシー権利法。
- D. カリフォルニア州プライバシー権法およびコロラド州プライバシー法。

Answer: C (メッセージを残す)

最新問題: 71

2012年の連邦取引委員会のレポート「急速な変化の時代における消費者のプライバシーの保護」に基づくと、次の指令のうち、企業にとって最も重要なものはどれですか。

- A. セキュリティ侵害後の消費者への被害を軽減します。
- B. データを収集する前に消費者がオプトインできるようにします。
- C. 製品開発中にプライバシー保護を統合します。
- D. 広告目的でオンライン行動を追跡することを発表します。

Answer: ([解答を表示する](#))

最新問題: 72

公正かつ正確な信用取引法 (FACTA) に基づく「レッドフラッグルール」は、送金サービスを利用する食料品店のオーナーとどのような関係がありますか？

- A. 信用記録を保護するために最新の技術の使用を義務付けている
- B. 所有者は個人情報盗難警告システムを実装する必要があります
- C. 小規模金融機関の場合、通常は適用されない
- D. 所有者は債権者ではないため適用されません

Answer: D ([メッセージを残す](#))

レッドフラッグルールは、金融機関および債権者に対し、対象口座の開設または既存の対象口座に関連する個人情報の盗難を検出、防止、および軽減するように設計された書面による個人情報盗難防止プログラムの実施を要求する規制です¹。債権者とは、定期的に信用を延長、更新、または継続する人、信用の延長、更新、または継続を定期的に手配する人、または信用の延長、更新、または継続の決定に参加する元の債権者の譲受人です²。対象口座とは、金融機関または債権者が主に個人、家族、または世帯の目的で提供または維持する口座で、複数の支払いまたは取引を伴うか、または許可するように設計されている口座で、クレジットカード口座、住宅ローン、自動車ローン、証拠金口座、携帯電話口座、公共料金口座、当座預金口座、または普通預金口座などです²。送金サービスは、顧客が電子的に送金または受け取りを行えるサービスです³。送金サービスを利用する食料品店のオーナーは、顧客への信用を定期的に延長、更新、継続していないため、債権者ではありません。したがって、送金サービスを利用する食料品店のオーナーにはレッドフラッグルールは適用されません。参考資料:

* 1: FTC、レッドフラッグルール、<https://www.ftc.gov/business-guidance/privacy-security/red-flags-rule>

* 2: FTC、「レッドフラッグルールによる個人情報盗難対策: ビジネス向けハウツーガイド」、<https://www.ftc.gov/tips-advice/business-center/guidance/fighting-identity-theft-red-flags-rule-how-guide-business>

* 3: Alessa、「電信送金の危険信号: マネーロンダリングと詐欺のリスクを理解する」、<https://alessa.com/webinars/wire-transfer-red-flags-and-fraud-risks/>

最新問題: 73

マサチューセッツ州個人情報セキュリティ規制では、個人情報の暗号化に関して何が求められていますか？

- A. すべての機器がマサチューセッツ州にある場合、マサチューセッツ州に拠点を置く企業に保存されているすべての個人情報を暗号化します。
- B. すべての機器がマサチューセッツ州にある場合、マサチューセッツ州居住者のすべての個人情報が暗号化されます。
- C. マサチューセッツ州に拠点を置く企業に保存されている個人情報をポータブル デバイスに保存する場合の暗号化。
- D. マサチューセッツ州居住者のすべての個人情報をポータブル デバイスに保存するときに暗号化します。

Answer: D ([メッセージを残す](#))

最新問題: 74

シナリオ

次の質問に回答するには、以下を使用してください。

ある晩、マットは息子の寝室に行き、息子がベッドに寝そべってノートパソコンを打っているのを見つけた。

「ネットワークを構築中ですか？」とマットは期待を込めて尋ねた。

「いいえ」少年は言った。「アンケートに答えているところです。」

マットは息子の肩越しに自分のコンピューターの画面を見た。「どんな調査？」私の意見についての質問だよ。」

「ちょっと見てみよう」とマットは言い、息子がすでに答えた質問のリストを読み始めた。政府と市民権についての意見を聞いているんだ。ちょっと変だな。君はまだ10歳なのに。」マットは、どうしてこのアンケートのウェblinkが息子のメールの受信箱に入ってしまったのか不思議に思った。このメッセージは息子に間違って送られたのかもしれないと思い、開いて読んでみた。このメッセージは、リーダーシップ プロジェクトという団体から送られてきたもので、内容と画像から子供向けであることがわかった。マットが読み進めると、アンケートに答えた子供は自動的に、有名なリーダーに関するシリーズの最初の本が当たるコンテストに登録されることがわかった。

マットにとって、これは明らかに子供たちに商品やサービスを売り込むためのマーケティング戦略に思えました。彼は息子に、アンケートに答えるために自分自身の情報を提供するよう求められたかどうか尋ねました。息子は、名前、住所、電話番号、生年月日を尋ねられ、好きなゲームやおもちゃについての質問に答えるよう求められたと答えました。

マットは心配していました。マーケティング担当者が息子からこのような方法で情報を収集することが合法かどうか疑問に思いました。その後、息子の受信箱に子供向けの商品を宣伝するマーケティング担当者からの他のいくつかの商業メールが届いていることに気づき、この事件を適切な当局に報告する時だと判断しました。

マーケティング担当者は、COPPA の「セーフハーバー」要件を満たすために、プライバシー管理プログラムをどのように変更するのが最善でしょうか。

- A. メールの内容についてFTCの承認を得ることにより
- B. COPPAプライバシー通知をウェブサイトで公開することにより
- C. 承認された自主規制プログラムに参加することにより
- D. 消費者のプライバシーに対するセキュリティリスクを定期的に評価することにより

Answer: C (メッセージを残す)

児童オンライン プライバシー保護法 (COPPA) は、オンライン サイトやサービスを利用する 13 歳未満の児童のプライバシーを保護する連邦法です。COPPA では、そのようなサイトやサービスの運営者に対し、児童から個人情報を収集、使用、または開示する前に、検証可能な保護者の同意を得ること、および保護者と一般の人々に情報慣行を通知することを義務付けています。また、COPPA では、保護者に児童の個人情報にアクセスし、確認、削除する権利、およびそのような情報のさらなる収集や使用を制限する権利を与えています。1 運営者が COPPA に準拠する方法の 1 つは、承認された自主規制プログラム (「セーフハーバー」プログラムとも呼ばれる) に参加することです。これらは、COPPA の要件を満たすかそれを超えるプライバシー保護の基準を設定および実施する業界グループまたはその他の組織によって運営されるプログラムです。

セーフハーバー プログラムに参加し、そのガイドラインに従う事業者は、COPPA に準拠しているとみなされ、FTC の執行措置ではなく、プログラムのレビューおよび懲戒手続きの対象となります。FTC は、CARU、ESRB、iKeepSafe、kidSAFE、PRIVO、TRUSTe など、いくつかのセーフハーバー プログラムを承認しています。2 承認された自主規制プログラムに参加することで、このシナリオのマーケティング担当者は、プライバシー管理プログラムを COPPA の「セーフハーバー」要件を満たすように変更するのが最善だった可能性があります。つまり、マーケティング担当者はプログラムのガイドラインに従う必要があり、これには、子供から個人情報を収集する前に検証可能な親の同意を得ること、Web サイトや電子メールで明確で目立つプライバシー通知を提供すること、子供のデータに関する親の選択と要求を尊重すること、収集されたデータのセキュリティと機密性を確保することなどが含まれる可能性があります。マーケティング担当者は、コンプライアンスの確保や苦情や紛争の解決において、プログラムの監視と支援を受けることもできます。3 参考文献: 1: COPPA への準拠: よくある質問4、セクション A2: COPPA セーフハーバー プログラム3: IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、143 ページ。

最新問題: 75

インターネットを介した児童への広告に関する法律を監督し、施行する機関はどれですか?

- A. 公民権局
- B. 連邦取引委員会
- C. 連邦通信委員会
- D. 国土安全保障省

Answer: B (メッセージを残す)

連邦取引委員会 (FTC) は、インターネットを通じて子供をターゲットにした広告やマーケティングの慣行を含む、米国の広告やマーケティング慣行を規制する主要な連邦機関です。FTC は、13 歳未満の子供を対象とした Web サイトやオンライン サービスの運営者に、子供から個人情報収集、使用、または開示する前に、検証可能な親の同意を得ることを義務付ける児童オンライン プライバシー保護法 (COPPA) を施行しています。また、FTC は、広告で虚偽または誤解を招く主張をするなど、商業における不公正または欺瞞的な行為や慣行を禁止する FTC 法も施行しています。FTC は、スポンサー コンテンツ、インフルエンサー、データ収集、説得力のあるデザイン、行動マーケティングなど、子供に対するデジタル広告のさまざまな側面に関するガイドラインとレポートを発行しています。FTC は、デジタル広告が子供に与える影響や、子供が広告と娯楽を区別する能力を調べるためのワークショップやイベントも主催しています。参考文献:

* FTCウェブサイト

* 子どもへのデジタル広告

* IAPP CIPP/US 学習ガイド、第 5 章: マーケティングとプライバシー、169-170 ページ

最新問題: 76

公正かつ正確な信用取引法 (FACTA) に基づく「レッドフラッグルール」は、送金サービスを利用する食料品店のオーナーとどのような関係がありますか?

- A. 信用記録を保護するために最新の技術の使用を義務付ける
- B. 所有者は個人情報盗難警告システムを実装する必要がある
- C. 小規模金融機関の場合、通常は適用されません。
- D. 所有者は債権者ではないため適用されません

Answer: A ([メッセージを残す](#))

有効な CIPP-US 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集! GoShiken.com が最新の CIPP-US 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (22830%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 77

グラム・リーチ・ブライリー法 (GLBA) が個人の銀行口座への不正アクセスを防止する主な方法は何ですか?

- A. セキュリティ侵害の疑いがある場合、直ちに公表を要求する。
- B. 金融機関に個人情報の収集を制限するよう要求する。
- C. 金融機関による顧客口座番号の開示を制限することにより。
- D. 顧客の個人情報を紙に印刷することを義務付けます。

Answer: ([解答を表示する](#))

最新問題: 78

米国では、どのような場合にデータ保護評価を実施するのがベストプラクティス（一部の州では必須）ですか？

- A. 採用プロセスの一環として身元調査が行われる場合
- B. 企業が情報を処理する場合。
- C. 企業秘密が第三者と共有される場合。
- D. 従業員を監視するためにテクノロジーが使用される場合。

Answer: D ([メッセージを残す](#))

米国では、従業員を監視するためにテクノロジーを使用する場合、データ保護影響評価 (DPIA) または同様の評価を実施することがベストプラクティスであり、一部の州では必須となっています。このプラクティスは、従業員のプライバシーへの潜在的な損害を最小限に抑えながら、監視プラクティスが適切で、必要かつ合法であることを保証することを目的としたプライバシー原則と一致しています。

従業員を監視する際に DPIA を実施する理由

* 従業員のプライバシー リスク: ビデオ監視、キーストロークの記録、位置追跡などの監視テクノロジーは、従業員のプライバシーに重大な影響を及ぼす可能性があります。評価は、これらのリスクを評価し、適用されるプライバシー法に準拠していることを確認するのに役立ちます。

* 州固有の要件: カリフォルニア州消費者プライバシー法 (CCPA) およびカリフォルニア州プライバシー権利法 (CPRPA) に基づくカリフォルニア州などの一部の州では、機密データに関連する高リスク活動の評価を含むプライバシー保護策を実施することを企業に義務付けています。

* ベストプラクティス: 法的に義務付けられていない場合でも、DPIA を実施することで説明責任が示され、従業員のプライバシー侵害に関連するリスクを軽減するのに役立ちます。

オプションの説明:

* A. 採用プロセスの一環として身元調査が行われる場合: 身元調査には機密データや公正信用報告法 (FCRA) などの法律への準拠が関係しますが、このプロセスでは通常 DPIA は必要ありません。代わりに、同意と通知が重視されます。

* B. 企業が情報を処理する場合: これは範囲が広すぎます。DPIA は一般に、機密データやテクノロジーに関連する高リスクのアクティビティにのみ適用され、すべてのデータ処理アクティビティに適用されるわけではありません。

* C. 企業秘密を第三者と共有する場合: 企業秘密の共有には契約および機密保持措置が含まれますが、個人データも含まれていない限り、通常はデータ保護評価は必要ありません。

* D. 従業員を監視するためにテクノロジーが使用される場合: 正解です。テクノロジーを使用して従業員を監視すると、プライバシーに重大なリスクが生じるため、プライバシーへの影響を評価し、州法および連邦法への準拠を保証することがベストプラクティス (場合によっては必須) となります。

CIPP/US 資料からの参照:

* カリフォルニア州プライバシー権法 (CPRA): 特定のデータ処理活動に対するリスク評価を導入します。

* IAPP CIPP/US 認定テキスト: 従業員の監視に関連するプライバシーのリスクと影響評価の重要性について説明します。

最新問題: 79

州の違反通知法では、個人情報の定義に通常含まれないものは何ですか？

- A. 州識別番号
- B. 名と姓
- C. 社会保障番号
- D. 医療情報

Answer: B (メッセージを残す)

州の侵害通知法では、個人情報は通常、個人のファーストネームまたはファーストネームの頭文字と姓に、社会保障番号、州識別番号、口座番号、医療情報などの1つ以上の他のデータ要素を加えたものと定義されています。ただし、ファーストネームと姓のみは、個人を特定したり、セキュリティやプライバシーを侵害したりする可能性のある他のデータ要素と組み合わせない限り、通常は個人情報とは見なされません。したがって、オプション B は、州の侵害通知法の下での個人情報の定義に通常は含まれていないため、正解です。参考文献:

<https://www.ncsl.org/technology-and-communication/security-breach-notification-laws>

<https://iapp.org/resources/article/state-data-breach-notification-chart/>

最新問題: 80

次の組織のうち、顧客に毎年プライバシー通知を提供する必要があるのはどれですか？

- A. フォーウィンズ部族大学。
- B. ゴールデン ギャベル オークションハウス。
- C. キング郡貯蓄貸付組合。
- D. ブリージーシティ住宅委員会。

Answer: C (メッセージを残す)

グラム・リーチ・ブライリー法 (GLBA) に基づく年次プライバシー通知要件は、例外要件を満たさない限り、顧客から非公開の個人情報を収集し、それを非関連第三者に開示する金融機関に適用されます。金融機関とは、1956年銀行持株会社法第4条(k)の定義に従い、本質的に金融的な活動またはそのような活動に付随する活動に従事する事業体です。キング郡貯蓄貸付金は、金銭の貸付と預金の受け入れを行っていることから、この定義に基づく金融機関です。したがって、例外要件を満たさない限り、顧客に年次プライバシー通知を提供する必要があります。フォーウィンズトライバルカレッジ、ゴールデンギャベルオークションハウス、およびブリージーシティ住宅委員会は、本質的に金融的な活動またはそのような活動に付随する活動に従事していないため、GLBAに基づく金融機関ではありません。

したがって、GLBAに基づいて顧客に毎年プライバシー通知を提供する必要はありません。

参考:

- * グラム・リーチ・ブライリー法第1条に基づく年次プライバシー通知要件の改正。背景、第2段落。
- * 17 CFR § 248.5 - 顧客への年次プライバシー通知の要求、パラグラフ (a) (1)。
- * IAPP CIPP/US 学習ガイド、65 ページ。

最新問題: 81

米国の州の半数以上がテレマーケティング業者に次のことを義務付けています。

- A. 通話の始めに自己紹介をする
- B. 潜在顧客から書面による同意を得る
- C. 事業を行う前に州に登録する
- D. 顧客取引に関する書面による契約を提供する

Answer: (解答を表示する)

IAPP CIPP/US 学習ガイドによると、米国の半数以上の州では、テレマーケティング業者が州内でビジネスを行う前に州に登録することを義務付けています。この登録要件には、料金の支払い、保証金の差し入れ、テレマーケティング業者の身元、所在地、ビジネス慣行に関する情報の提供などが含まれる場合があります。この要件の目的は、詐欺的または欺瞞的なテレマーケティングの電話から消費者を保護し、州の法律や規制の施行を促進することです。その他のオプションはほとんどの州で義務付けられていませんが、一部の州では身元確認、同意、契約に関してテレマーケティング業者向けの追加の規則やガイドラインが定められている場合があります。参考文献:

- * IAPP CIPP/US 学習ガイド、第7章: マーケティングと広告
- * 州のテレマーケティング登録要件

最新問題: 82

連邦取引委員会法の本来の目的は何でしたか?

- A. 米国民のプライバシー権を確保するため
- B. 消費者を保護するため
- C. 独占禁止法を施行するため
- D. 個人のプライバシーを侵害する企業との同意判決の交渉

Answer: C (メッセージを残す)

連邦取引委員会法 (FTCA) は、米国経済における独占とトラストの権力と影響力を抑制することを目的とした進歩主義時代の改革の一環として 1914 年に採択されました。FTCA は、不公正な競争方法や、商業におけるまたは商業に影響を与える不公正または欺瞞的な行為や慣行を調査および防止する独立機関として連邦取引委員会 (FTC) を設立しました。また、FTCA は、FTC に、法律違反に対する停止命令の発行、差し止め命令の請求、民事罰の適用の権限を与えました。FTCA は、取引の制限、価格協定、合併、その他の反競争行為を禁止するシャーマン法やクレイトン法などの既存の反トラスト法を補完および補足することを目的としていました。

他のオプションは正しくありません。理由は次のとおりです。

* FTCA は米国市民のプライバシー権について明示的には言及していませんでしたが、FTC は後に FTCA に基づく権限を使用して、虚偽または誤解を招く主張を行うこと、重要な情報を開示しないこと、個人データに関する消費者の選択や期待に反することなど、不公正または欺瞞的なプライバシー慣行を強制しました。

* FTCA は消費者保護に特に焦点を当てていませんでした。しかし、FTC は後にその範囲を拡大し、広告とマーケティング、信用と金融、プライバシーとセキュリティ、消費者教育などの消費者保護問題も対象としました。FTC は、貸付に関する真実の法、公正信用報告法、児童オンライン プライバシー保護法、CAN-SPAM 法など、その他の消費者保護法も施行しました。

* FTCA は、FTC が個人のプライバシーを侵害する企業と同意判決を交渉することを認めていませんが、FTC は後に同意判決をプライバシー訴訟の解決や、監査、報告書、コンプライアンス プログラムなどの是正措置の実施に共通のツールとして使用しました。同意判決とは、FTC と訴訟の当事者間の合意であり、責任や不正行為を認めずに FTC の告発を解決するものです。

参考文献:

* FTCウェブサイト、連邦取引委員会法

* ブリタニカのウェブサイト、連邦取引委員会法 (FTCA)

* IAPP CIPP/US 学習ガイド、第 1 章: 米国のプライバシー環境の概要、11 ~ 12 ページ

* IAPPウェブサイト、連邦取引委員会法第5条

最新問題: 83

外国情報監視法の本来の目的は何でしたか?

- A. 公立図書館でのインターネット アクセスなど、米国愛国者法に基づいて公共の場所で合理的に監視できる情報をさらに定義します。
- B. 憲法第2条に基づき、国家安全保障の目的で行政機関による盗聴を許可するための枠組みをさらに定義する。
- C. Katz v. United States 判決から生じるプライバシーの合理的な期待をさらに明確にします。
- D. Olmstead v. United States の判決に基づき、電話会社が容疑者の自宅外で内部的に盗聴を行う場合に令状が必要ない場合についてさらに明確にします。

Answer: A (メッセージを残す)

最新問題: 84

米国の民間部門の従業員にプライバシー保護を提供する可能性が最も高いのは次のどれですか?

- A. 州法、契約法、不法行為法
- B. 連邦取引委員会法 (FTC法)
- C. アメリカ合衆国憲法修正第1条、第4条、第5条
- D. 米国保健福祉省 (HHS)

Answer: A (メッセージを残す)

説明/参照: <https://corporate.findlaw.com/law-library/right-to-privacy-in-the-workplace-in-the-information-age.html>

最新問題: 85

データ侵害通知法を制定しているほとんどの州では、影響を受けた個人への通知は、「不当な遅延なく可能な限り迅速に」。対照的に、影響を受ける個人への通知に明確な制限を現在課している州は次のどれですか。

- A. メイン
- B. フロリダ
- C. ニューヨーク
- D. カリフォルニア

Answer: B ([メッセージを残す](#))

説明/参照: <https://www.itgovernanceusa.com/data-breach-notification-laws>

最新問題: 86

対象事業体が、500人以上の個人の個人健康情報 (PHI) に影響を及ぼすランサムウェア攻撃を受けました。HIPAA に基づく連邦法によれば、対象事業体が侵害を報告する必要がないのは次のどれですか。

- A. 地元メディア
- B. 影響を受けた個人
- C. 医療提供者
- D. 保健福祉省

Answer: C ([メッセージを残す](#))

最新問題: 87

金融機関は、マーケティング目的で消費者情報を非関連第三者と共有できるのはどのような場合ですか？

- A. 情報共有の慣行を顧客に開示し、顧客にオプトインの機会を与えた後。
- B. 顧客にマーケティング手法を開示し、オプトインする機会を与えた後。
- C. 情報共有の慣行を顧客に開示し、顧客にオプトアウトの機会を与えた後。
- D. 顧客にマーケティング手法を開示し、オプトアウトする機会を与えた後。

Answer: (解答を表示する)

グラム・リーチ・ブライリー法 (GLBA) およびその実施規則 P によれば、金融機関は、情報共有の慣行を顧客に開示し、顧客にそのような共有をオプトアウトする機会を与えた後のみ、マーケティング目的で非関連第三者と消費者情報を共有できます。GLBA では、顧客を、主に個人、家族、または世帯の目的で使用される 1 つ以上の金融商品またはサービスを提供する金融機関と継続的な関係を持つ消費者と定義しています。消費者とは、主に個人、家族、または世帯の目的で使用される金融商品またはサービスを金融機関から取得している、または取得した個人、またはその個人の法定代理人です。非関連第三者とは、金融機関の関連会社、または金融機関と金融機関の関連会社ではない会社によって共同で雇用されている人を

除くすべての人です。関連会社とは、別の会社を支配する、別の会社に支配される、または別の会社と共同で支配される会社です。

GLBA では、金融機関が顧客にプライバシー通知を次の場合に提供することが義務付けられています。(i) 顧客関係を確立したとき、(ii) 顧客関係の継続中は毎年、(iii) 例外が適用されない限り、顧客に関する非公開個人情報 (NPI) を非関連第三者に開示する前に。プライバシー通知には、金融機関が収集および開示する NPI のカテゴリ、金融機関が NPI を開示する関連会社および非関連第三者のカテゴリ、サービス プロバイダーおよび共同マーケティング担当者に開示される NPI のカテゴリ、NPI の機密性とセキュリティの保護に関するポリシーと慣行、および顧客がオプトアウトする権利を持つ NPI の開示について記載する必要があります。金融機関は、チェックボックス、返信フォーム、フリーダイヤル番号など、顧客が非関連第三者への NPI の開示をオプトアウトするための合理的な手段も提供する必要があります。オプトアウト通知は明確かつ目立つものでなければならず、顧客がいつでもオプトアウトできることを明記する必要があります。オプトアウト通知では、顧客がオプトアウトする方法とオプトアウトの影響についても説明する必要があります。金融機関は、顧客のオプトアウト指示を受け取った後、合理的に実行可能な限り速やかにその指示を尊重しなければならず、例外が適用されない限り、オプトアウトが適用される NPI を公開してはなりません。GLBA では、オプトアウト要件にいくつかの例外が設けられています。たとえば、顧客が要求または承認した取引を実行、管理、または強制するために NPI の開示が必要な場合、法律で NPI の開示が要求または許可されている場合、公正信用報告法に従って消費者報告機関に NPI を開示する場合、または共同マーケティング契約に基づき金融機関に代わって、または金融機関と別の金融機関に代わってマーケティング サービスを実行する人物に NPI を開示する場合などです。共同マーケティング契約は、金融機関とその他の人物との間の正式な書面による契約であり、当事者は金融商品またはサービスを提供、推奨、または後援することに合意します。共同マーケティング契約では、契約の対象となる金融商品またはサービスを提供、推奨、または後援する以外の目的で、相手方が NPI を使用または開示することを禁止する必要があります。

GLBA では、例外が適用されない限り、金融機関は、顧客ではない消費者に関する NPI を非関連第三者に開示する前に、顧客ではない消費者にプライバシー通知を提供することも義務付けています。金融機関は、顧客ではない消費者と顧客関係がない限り、顧客ではない消費者にオプトアウト通知を提供する必要はありません。ただし、金融機関が以前は顧客ではなかった消費者と顧客関係を確立する場合は、上記のように、顧客にプライバシー通知とオプトアウト通知を提供する必要があります。

参考文献:

* グラム・リーチ・ブライリー法ガイド

* GLBA か FCRA か? 関連会社と非関連会社間のデータ共有

* 既存のプライバシー法では既に情報共有が規制されている

* 銀行があなたの財務情報を共有するのはなぜですか? また、それは許可されていますか?

* [IAPP CIPP/US 認定情報プライバシー専門家学習ガイド]、第 5 章、161 ~ 165 ページ。

最新問題: 88

1984 年のケーブル通信政策法では、どの活動が義務付けられていますか？

- A. 加入者情報の使用方法を詳述した年次通知の配信
- B. ケーブルサービスを提供するために必要な個人情報を配布するための加入者の同意を得る
- C. 個人情報は、不要になった後、最大6か月以内に破棄されます。
- D. ケーブルサービスの不正受信に関する調査について加入者に通知

Answer: D (メッセージを残す)

最新問題: 89

チャンネルヘアスタジオは、忙しい高級ヘアサロンです。業務の効率を最大限に高め、予約の待ち時間を短縮するために、チャンネルは、顧客プロフィールと履歴を使用して、どの顧客が予約に遅れる可能性が高いかを予測する人工知能ソフトウェアを導入することにしました。顧客プロフィールを作成するために使用された情報には、予約履歴、サロンからの距離、顧客のソーシャルメディアアカウントから取得された遅刻に関する言及が含まれます。顧客が遅れると予測された場合、その顧客の予約は5分以内にキャンセルされます。

詳細を踏まえると、チャンネルによるこの新しいソフトウェアの使用に関連する最大の潜在的なプライバシーの懸念は何でしょうか？

- A. 予測目的でサロンの顧客の遅刻履歴を評価します。
- B. 予約の設定以外の目的でクライアントのプロファイル情報を使用する。
- C. クライアントに通知せずにクライアントのソーシャルメディアアカウントをスキャンし、クライアントプロフィールで使用します。
- D. サロンからのクライアントプロフィールの住所の距離を計算して、サロンからの位置を特定し、クライアントが遅れるかどうかを予測します。

Answer: D (メッセージを残す)

最新問題: 90

次の州のうち、生体認証データの収集を具体的に規制する法律を制定した最初の州はどれですか？

- A. カリフォルニア。
- B. テキサス。
- C. イリノイ州。
- D. ワシントン。

Answer: C (メッセージを残す)

イリノイ州は、2008年にバイオメトリック情報プライバシー法 (BIPA) を制定し、バイオメトリックデータの収集を具体的に規制する法律を可決した最初の州となりました。BIPAでは、バイオメトリック識別子を網膜または虹彩のスキャン、指紋、声紋、または手や顔の形状のスキャンと定義し、バイオメトリック情報を、個人を識別するために使用されるバイオメトリック識別子に基づく情報と定義しています。BIPAでは、バイオメトリック識別子または情報を収集、保存、または使用する組織に対して、個人からインフォームドコンセントを取

得し、データの保持と破棄に関する書面によるポリシーを提供し、バイオメトリック データの開示と販売を制限し、適切なセキュリティ対策を使用してバイオメトリック データを保護することを義務付けています。BIPA はまた、生体認証データが法律に違反して収集、保管、または使用された個人に民事訴訟権を与え、過失による違反ごとに 1,000 ドルまたは実際の損害額のいずれか大きい方の法定損害賠償、故意または無謀な違反ごとに 5,000 ドルまたは実際の損害額のいずれか大きい方の法定損害賠償、および弁護士費用と経費、差し止め命令による救済を請求できるようにします。参考文献: 米国の生体認証法パート I: 2020 年の概要、生体認証情報はプライバシー法で保護されていますか?、生体認証データのプライバシー法

最新問題: 91

米国最高裁判所は、次のどれを認めることにより、避妊などの個人的な問題に関する個人のプライバシーの権利を認めましたか?

- A. 個人のプライバシー権を明示的に認めている州憲法を連邦政府が優先すること。
- B. 列挙されていない憲法上の権利の「周辺領域」、および適正な法的手続きによるより一般的な保護。
- C. 個人的な問題にまで及ぶ米国憲法の明示的なプライバシーの定義の解釈。
- D. 先例拘束の原則。これにより、米国最高裁判所は以前に決定された判例の先例に従うことができます。

Answer: B (メッセージを残す)

米国最高裁判所は、「列挙されていない憲法上の権利の 周辺領域」と、より一般的な適正手続きの保護を認めることにより、避妊などの個人的な問題に関する個人のプライバシー権を認めてきました。これは、プライバシー権が憲法に明示的には規定されていないが、明示的に規定されている他の権利、たとえば、憲法修正第 1 条の言論および集会の権利、憲法修正第 3 条の兵役免除の権利、憲法修正第 4 条の不当な搜索および押収からの保護、憲法修正第 5 条の自己負罪免除の権利、憲法に列挙されていないその他の権利を保持する憲法修正第 9 条の権利から暗黙的に規定されていることを意味します。これらの権利は、個人が個人の事柄に不当に干渉する政府から個人を保護する「プライバシー領域」を作り出します。最高裁判所は、グリスウォルド対ジョージ・ブッシュ事件で初めてこのプライバシーの概念を明示しました。

コネチカット州 (1965 年) では、結婚したカップルによる避妊具の使用を禁じる州法を無効としました。最高裁はまた、州が法の適正手続きなしに人の生命、自由、財産を奪うことを禁じる、合衆国憲法修正第 14 条の適正手続き条項にも依拠しました。最高裁はこの条項を、州のやむを得ない利益があり、その利益を達成するために規制が厳密に調整されている場合を除き、州の規制から特定の基本的権利を保護する実質的な要素を含むと解釈しました。最高裁はこの適正手続き分析を、中絶、結婚、性的指向などの他のプライバシー問題に適用しました。参考文献:

* プライバシー | Wex | 米国法 | LII / 法律情報研究所

* プライバシーは憲法には規定されていないが、憲法上のあらゆるところに存在している

* プライバシー権と個人の自治は...によって法的に保護されています - Justia

* プライバシーの権利 | Wex | 米国法 | LII / 法律情報研究所

有効な **CIPP-US** 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集！ GoShiken.com が最新の **CIPP-US** 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (**22830%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 92

プライバシー法に基づく個人の開示の権利から免除される資料の種類は何ですか？

- A. 資料は法律により研究目的にのみ維持および使用することが義務付けられています。
- B. 個人に対する不法な迫害を防ぐための調査活動を報告する資料。
- C. 貿易協定の交渉において外国政府との潜在的な協力関係を判断するために使用される資料。
- D. 刑法の執行に関連する調査活動を報告する資料。

Answer: B (メッセージを残す)

<https://www.dea.gov/foia/privacy-act-exemptions>

最新問題: 93

どのような状況で「消費者に選択肢を与えない」または「オプションを与えない」という政策が予想されるでしょうか？

- A. 求職者の信用報告書が雇用主に提供される場合
- B. 政府から顧客の財務情報が要求された場合
- C. 患者の健康記録が製薬会社に提供される場合
- D. 顧客の住所が配送会社と共有される場合

Answer: D (メッセージを残す)

たとえば、オンラインで商品を注文する消費者は、配送会社、クレジットカード処理業者、および取引の履行に携わるその他の関係者と個人情報共有されることを期待しています。消費者は、配送会社が住所を知るためにオプトインに署名したり、オプトアウトのオプションを提供されたりすることを予想していません」IAPP_US_TB_US-Private-Sector-Privacy-3E_1.0 からの抜粋

最新問題: 94

1984年のケーブル通信政策法では、どの活動が義務付けられていますか？

- A. 加入者情報の使用方法を詳述した年次通知の送付
- B. 個人情報は、不要になった後、最大6か月以内に破棄されます。

C. ケーブルサービスの不正受信に関する調査について加入者に通知

D. ケーブルサービスを提供するために必要な個人情報を配布するための加入者の同意を得る

Answer: A (メッセージを残す)

1984 年ケーブル通信政策法 (CCPA) は、ケーブルテレビ業界を規制し、ケーブル加入者のプライバシーを保護する連邦法です。CCPA の規定の 1 つに、ケーブル事業者は加入者に次の情報を明確かつ目立つ形で通知する年次通知を提供しなければならないというのがあります¹²。

* 加入者に関して収集される、または収集される予定の個人情報の性質、およびそのような情報の使用の性質

* 当該情報の開示の性質、頻度、目的、開示対象となる人物の種類の特定を含む

* ケーブル事業者がそのような情報を保持する期間

* 加入者がそのような情報にアクセスできる時間と場所

* ケーブル事業者による情報の収集および開示に関して CCPA が定める制限、および CCPA に基づく加入者のそのような制限を強制する権利。年次通知には、加入者が法律または裁判所命令で要求される場合を除き、個人情報の第三者への開示を防止する権利を有すること、および加入者が CCPA 違反に対する損害賠償、弁護士費用、およびその他の救済を求めて訴訟を起こすことができることも記載する必要があります¹²。

参考文献: 1: 1984 年ケーブル通信政策法、第 631 条 2: [IAPP CIPP/US 学習ガイド]、第 8 章、第 8.3.2 項

最新問題: 95

シナリオ

次の質問に回答するには、以下を使用してください。

あなたは、米国 A 州の大都市にある大規模病院、HealthCo の最高プライバシー責任者です。HealthCo は HIPAA の対象事業体であり、100,000 人以上の患者に医療サービスを提供しています。サードパーティのクラウドコンピューティング サービス プロバイダーである CloudHealth は、HealthCo に代わってこれらの個人の電子保護医療情報 (ePHI) を保存および管理しています。CloudHealth はデータを状態 B に保存します。

HealthCo と CloudHealth とのビジネス アソシエート契約 (BAA) の一環として、HealthCo は CloudHealth に対し、データを適切に保護するために業界標準の暗号化手法を含むセキュリティ対策を実施することを要求しています。しかし、HealthCo は契約締結前に CloudHealth に対してデューデリジェンスを実施しておらず、CloudHealth のセキュリティ対策の監査も実施していません。

CloudHealth の従業員が最近フィッシング攻撃の被害者になりました。従業員が不審なメールのリンクをうっかりクリックしたため、HealthCo の患者 10,000 人以上の PHI が侵害され、その後、その情報がオンラインで公開されました。HealthCo のサイバーセキュリティチームは、犯人が他の病院に対して同様の攻撃を仕掛けた既知のハッカーであることをすぐに特定しました。この攻撃では、著名人や政治家などの公人の PHI が漏洩しました。

調査の過程で、HealthCo は、CloudHealth が契約条件に従って PHI を暗号化していなかったことを発見しました。さらに、CloudHealth は従業員にプライバシーやセキュリティに関するトレーニングを提供していませんでした。法執行機関は、HealthCo に対し、侵害に関する調査報告書と影響を受けた個人の PHI のコピーを提供するよう要求しました。

侵害の影響を受けた患者は、HealthCo 社が患者の ePHI を適切に保護しなかったため、漏洩したデータによって患者が多大な損害を被ったと主張して同社を訴えました。患者の弁護士は、侵害で漏洩した ePHI に関する証拠開示請求を提出しました。

HIPAA セキュリティ ルールで要求される安全対策のうち、HealthCo の行動によって問題にならないのは次のどれですか。

- A. 技術的安全対策
- B. 管理上の安全策
- C. 物理的な安全対策
- D. セキュリティ保護

Answer: D (メッセージを残す)

最新問題: 96

2012 年 3 月、FTC は消費者データを扱う企業のための 3 つの基本原則を概説したプライバシー レポートを発表しました。これらの原則のうち、どれではないでしょうか。

- A. 透明性を高めます。
- B. セキュリティ対策の強化。
- C. 消費者の選択を簡素化します。
- D. プライバシーバイデザインを実践する。

Answer: B (メッセージを残す)

最新問題: 97

連邦法および州法に基づくデータ侵害通知に関して、最も正確な記述は次のうちどれですか。

- A. 500 人を超える個人が通知を受け取る場合は、影響を受ける個人に加えて連邦取引委員会 (FTC) にも通知する必要があります。
- B. 個人に対してデータ侵害の必要な通知を提供する場合、実際に侵害された、または侵害された可能性のある個人情報に特定する必要があります。
- C. 州法に基づいて個人にデータ侵害の通知を提供することが義務付けられている場合は、個人に無料の信用監視のオファーを提供する必要があります。
- D. 現在、個人情報の漏洩に関する通知を義務付ける連邦法や規制がないため、データ漏洩通知の義務は州法の下にのみ存在します。

Answer: D (メッセージを残す)

米国におけるデータ侵害通知法は州や地域によって異なり、すべての種類の個人情報に適用される包括的な連邦法はありません。HIPAA、GLBA、FDIC 規則など一部の連邦法では、特定の業界やセクターに対してデータ侵害通知要件を課していますが、すべての種類の個人情報

報や、そのような情報を収集、保存、または処理するすべての組織を対象としているわけではありません。

したがって、特定の連邦法が当該団体または関連する情報に適用されない限り、個人情報の漏洩に関するデータ漏洩通知を提供する義務は州法のみにあります。その他の記述は、以下の理由により誤りです。

* A. 500 人を超える個人が通知を受ける場合、影響を受ける個人に加えて FTC に通知する必要はありません。ただし、HIPAA の対象となる医療機関の場合は、侵害から 60 日以内に保健福祉省 (HHS) に通知する必要があります。

* B. 個人に対してデータ侵害の必要な通知を提供する場合、州法で義務付けられていない限り、実際に侵害された、または侵害された可能性のある個人情報を特定する必要はありません。

カリフォルニア州など一部の州では、通知に、漏洩の対象となった、または漏洩の対象となったと合理的に考えられる個人情報の種類を含めることを義務付けていますが、アラバマ州など他の州では、通知の内容を指定していません。

* C. 州法に基づいて個人にデータ侵害の通知をする必要がある場合、州法で義務付けられていない限り、個人に無料の信用監視を提供する必要はありません。コネチカット州など一部の州では、少なくとも 12 か月間、適切な個人情報盗難防止および軽減サービスの提供を義務付けていますが、アリゾナ州など他の州では、そのような義務は課していません。参考資料: 米国および領土におけるデータ侵害通知、米国のデータ侵害通知法: 必要な内容とその決定方法、米国州データ侵害通知法マトリックス、米国における侵害通知、データ侵害通知法: 自信を持って対応する方法

最新問題: 98

次の州法のうち、グラム・リーチ・ブライリー法 (GLBA) の対象となる組織に対して法人免除が定められているのはどれですか?

- A. ネバダ州プライバシー法。
- B. カリフォルニア州プライバシー権利法。
- C. カリフォルニア州消費者プライバシー法。
- D. バージニア州消費者データ保護法

Answer: ([解答を表示する](#))

しかし、VCDPA は金融機関には適用されません。具体的には、VCDPA は「連邦 GLBA のタイトル V の対象となる金融機関またはデータには適用されない」と規定しています。この点で、VCDPA の GLBA 例外は、GLBA の対象となる情報のみに限定されている CCPA の GLBA 例外よりもはるかに広範囲です。つまり、CCPA とは異なり、VCDPA は「GLBA 情報」例外だけでなく、GLBA 「エンティティ」例外も提供しています。」

<https://www.mofo.com/resources/insights/210302-financial-institutions-exempt-virginia-privacy-law>

最新問題: 99

FERPA によれば、学校はどのような場合に生徒の同意なしに記録を開示できるのでしょうか？

- A. 開示が第三者への電子メールを通じて行われない場合
- B. 開示によって学生の学生番号が明らかにならない場合
- C. 学生の健康管理に携わる医療従事者への開示の場合
- D. 開示が、学生が入学を希望する学校に成績証明書を提供することである場合

Answer: D (メッセージを残す)

説明/参照: <https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>

最新問題: 100

シナリオ

次の質問に回答するには、以下を使用してください。

ラリーは、サンライズリンクスでのテレマーケティングの職務、特に上司のエヴァンにますます不満を募らせている。先週、エヴァンが州の Do Not Call リストとそこに載っている人々をあざ笑っているのを耳にした。迷惑をかけたくないと本気で思っているなら、全国 DNC リストに載っているはずだ。それが私たちが従わなければならない唯一のリストだ。サンライズリンクスでは、「電話しないでほしいと言われるまで電話をかけ続ける」。奇妙なことに、エヴァンはテレマーケティング担当者に、「受信者が 別の機会に」電話してほしいと頼んだ場合の記録を残すよう要求している。ラリーにとって、これは彼らがまったく電話を受けたくないという明らかな兆候だ。エヴァンはそうは考えていない。

ラリーは、エヴァンの傲慢さが従業員への接し方にも影響していると考えています。米国憲法は米国の労働者を保護しており、ラリーはサンライズリンクスの従業員の権利が定期的に侵害されていると考えています。最初、エヴァンはソーシャルメディアで従業員と交流するなど、友好的に見えました。しかし、エヴァンの政治的な投稿を見て、昇進を申し出られるのは同じような立場の従業員だけであることがラリーには明らかになりました。

さらに、ラリーは時々、私的使用の品が入った小包を職場に郵送してもらっています。名前がはっきり記されているにもかかわらず、すでに開封された状態で届いたことが何度かありました。ラリーは、サンライズリンクスでは私的郵便物の開封は一般的であり、エヴァンのリーダーシップの下では憲法修正第 4 条の権利が踏みにじられていると考えています。

ラリーは同僚のセイディーに関する会話を耳にして落胆したこともある。テレマーケティングの電話は品質保証のために定期的に録音されており、セイディーは仕事中は常にプロフェッショナルだが、私的な会話には性的な発言が含まれることがある。ラリーはエヴァンがこれについても笑っているのを聞いたことがある。彼が同僚にこのことを話すと、彼の懸念は肩をすくめるだけで済んだ。同僚は、従業員は入社時に監視されることに同意していると思っていた。個人のデバイスには手を付けていないが、電話、メール、閲覧履歴はすべて監視対象となっている。実際、ラリーは、外部の会社による覆面調査で不正行為の証拠が見つかり、従業員が解雇された事例を 1 件知っている。その従業員は会社から盗んだのかもしれないが、エヴァンは何かおかしいと最初に疑った時点で当局に連絡すればよかったのだ。

ラリーは行動を起こしたいと思っていますが、どのように進めればよいかわかりません。

どの行為がエヴァンの潜入捜査を許可するでしょうか？

- A. 内部告発者保護法
- B. 保存通信法 (SCA)
- C. 全国労働関係法 (NLRA)
- D. 公正かつ正確な信用取引法 (FACTA)

Answer: [\(解答を表示する\)](#)

保存通信法 (SCA) は、電子メール プロバイダー、クラウドストレージ プロバイダー、ソーシャル メディア プラットフォームなどのサードパーティ サービス プロバイダーによって保存される電子通信のプライバシーを規制する連邦法です。SCA は、法律で許可されている場合、またはユーザーやサービス プロバイダーの同意がある場合を除き、そのような通信への不正アクセスや開示を禁止しています。また、SCA は、法執行目的、サービス プロバイダーの権利や財産の保護、加入者や顧客の同意など、特定の種類のアクセスや開示に対しては例外を設けています。

SCA の例外の 1 つは、サービス プロバイダーが保存された通信へのアクセスまたは開示に同意する場合です。つまり、サードパーティのサービス プロバイダーが調査または情報要求に協力することに同意した場合、そのアクセスまたは開示は SCA の下で合法です。同意は、状況とプロバイダーの利用規約に応じて、明示的または暗黙的になります。たとえば、サービス プロバイダーが正当な目的でユーザー情報をサードパーティに開示することを許可するポリシーを持っている場合、プロバイダーは保存された通信へのアクセスまたは開示に暗黙的に同意しています。ただし、サービス プロバイダーがそのような開示を禁止するポリシーを持っている場合、プロバイダーは保存された通信へのアクセスまたは開示に同意していません。

このシナリオでは、エヴァンの潜入捜査は、不正行為の疑いのある従業員の電子通信を保存しているサードパーティのサービスプロバイダーの同意を得ていれば、SCA によって承認されていた可能性があります。たとえば、従業員が会社のメールアカウントやクラウドストレージサービスを使用していて、そのサービスプロバイダーがユーザー情報を雇用主や法執行機関に開示することを許可するポリシーを持っていた場合は、エヴァンはサービスプロバイダーの同意を得て、保存されている通信にアクセスしたり開示したりできた可能性があります。しかし、従業員が個人のメールアカウントやクラウドストレージサービスを使用していて、ユーザーのプライバシーを保護し、そのような開示を禁止するポリシーを持っていた場合は、エヴァンはサービスプロバイダーの同意なしに保存されている通信にアクセスしたり開示したりすることで、SCA に違反した可能性があります。

参考文献: [蓄積通信法]、18 USC §§ 2701-2712 : [IAPP CIPP/US 学習ガイド]、第 8 章、セクション 8.2.2。: [蓄積通信法: 現代の問題に対する古い法律]、pp. 10-11.

最新問題: 101

シナリオ

次の質問に回答するには以下を使用してください

大手小売店で顧客の個人情報と財務情報に関するデータ漏洩が発生したとき、会社の役員たちは衝撃を受けました。しかし、同社のプライバシーアナリストであり、自身も個人情報盗難の被害者であるロベルタは衝撃を受けませんでした。漏洩が発生する前、彼女は役員向けのプライバシープログラムレポートに取り組んでいました。会社が組織全体でデータを共有し、処理する方法が大きな懸念事項でした。顧客情報へのアクセスに関する適切なルールも、古くなったデータを消去および破棄する手順もありませんでした。ロベルタは調査で、下級従業員でさえ会社のすべての顧客データ（財務記録を含む）にアクセスでき、会社には1980年代にさかのぼる古い顧客データがまだ残っていることを発見しました。

彼女の報告書は、3つの主要な改革を推奨しています。まず、必要に応じてアクセスを許可すること。これは、従業員が顧客情報にアクセスすることを、業務に関連するデータのみで制限することを意味します。

次に、顧客の財務情報（クレジットカード番号や銀行口座番号など）を機密性の低い情報とは別に保管するための、非常に安全なデータベースを作成します。最後に、古くなった顧客情報を特定し、それを安全に廃棄するプロセスを開発します。

侵害が発生したとき、同社の幹部はロベルタを会議に招集し、彼女は報告書で推奨事項を提示しました。ロベルタは、同社が全国規模の顧客基盤を持つということは、関連するすべての州の侵害通知法に準拠する必要があることを説明しました。ロベルタの指導のおかげで、同社は州の侵害通知法で定められた特定の時間枠内で迅速に顧客に通知することができました。

その後すぐに、役員らはロベルタが報告書で推奨したプライバシープログラムの変更を承認しました。これらの変更により、またプライバシーとセキュリティがすべての従業員の責任とみなされるようになったことにより、プライバシープログラムははるかに効果的になりました。

ロベルタが指摘した同社のプライバシーセキュリティの問題に基づくと、侵害の最も可能性の高い原因は何でしょうか？

- A. アクセス制御の欠如による情報の不適切な取り扱い。
- B. 第三者と共有された情報の意図しない開示。
- C. POS端末でのクレジットカード盗難を伴う詐欺。
- D. コンピューターやフラッシュドライブなどの会社の資産を紛失しました。

Answer: A (メッセージを残す)

このシナリオでは、会社が顧客情報へのアクセスに関する適切なルールを定めておらず、下位レベルの従業員が財務記録を含む会社のすべての顧客データにアクセスできたことが説明されています。これは、会社が役割と責任に基づいて顧客情報にアクセス、使用、開示できるユーザーを制限する適切なアクセス制御を実装していなかったことを示しています。アクセス制御は、機密データへの不正または不適切なアクセスを防ぐのに役立つため、情報セキュリティとプライバシーの重要な要素の1つです。

アクセス制御がなければ、同社の顧客情報は、セキュリティ対策の弱点を悪用する従業員や部外者による不適切な取り扱いに対して脆弱でした。したがって、侵害の原因として最も可能性が高いのは、アクセス制御の欠如による情報の不適切な取り扱いです。参考資料:

* IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第 4 章: 米国の観点からの情報管理、セクション 4.2: 情報セキュリティ、p. 113-114

* IAPP CIPP/US Body of Knowledge、ドメイン I: 米国のプライバシー環境の概要、目標 I.C: プライバシーにおける情報セキュリティの役割を説明する、サブ目標 IC1: 情報セキュリティの主要要素を特定する、p. 8

最新問題: 102

未承諾ポルノおよびマーケティング攻撃規制法 (CAN-SPAM) は、どのような点で消費者を支援することを目的としていますか？

- A. 企業に、消費者が今後の電子メールの受信を拒否できるように義務付けることによって。
- B. 消費者に無料のスパムフィルタリングソフトウェアを提供します。
- C. 企業が迷惑メールを通じて不快なコンテンツを送信することを禁止する。
- D. 広告メールを送信する前に、企業がオプトインを受信することを義務付けます。

Answer: ([解答を表示する](#))

最新問題: 103

次の連邦機関のうち、公正かつ正確な信用取引法 (FACTA) に基づく廃棄規則を施行しないのはどれですか？

- A. 消費者金融保護局
- B. 保健福祉省
- C. 通貨監督庁
- D. 連邦取引委員会

Answer: B ([メッセージを残す](#))

最新問題: 104

次の連邦機関のうち、プライバシーに関する規制権限を持たないのはどれですか？

- A. 米国商務省。
- B. 消費者金融保護局。
- C. 連邦準備制度
- D. 米国運輸省。

Answer: ([解答を表示する](#))

最新問題: 105

アジア太平洋経済協力 (APEC) の原則を最もよく表しているのはどれですか？

- A. オプトアウト メカニズムを提供するマーケティング担当者の最低限の責任のベースライン。
- B. 医療機関がプライバシー法を遵守するための責任規定。
- C. 個人情報へのアクセスを求める個人の権利章典。
- D. 商業分野で保有される個人情報に関する国際裁判所の判決。

Answer: C ([メッセージを残す](#))

最新問題: 106

連邦取引委員会法の本来の目的は何でしたか?

- A. 米国民のプライバシー権を確保するため
- B. 消費者を保護するため
- C. 独占禁止法を施行するため
- D. 個人のプライバシーを侵害する企業との同意判決の交渉

Answer: C ([メッセージを残す](#))

IAPP ブック、セクション 3.3、最初の文。FTC は、独占禁止法を施行するために 1914 年に設立され、その一般的な消費者保護の使命は 1938 年の法改正によって確立されました。」特にこの回答を検討する際には、FTC 法が最初に可決されたのは 1914 年であることに留意してください。

有効な CIPP-US 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集! GoShiken.com が最新の CIPP-US 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (22830%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 107

テレマーケティング販売規則では、組織全体で電話禁止要求を共有することがいつ義務付けられるのでしょうか?

- A. 部門が販売する商品やサービスが非常に類似している場合
- B. 部門の運営体制が透明でない場合
- C. 呼び出しがエラーやその他の予期しない原因によるものではない場合
- D. エンティティが複数のプラットフォームを通じてユーザーの設定を管理する場合

Answer: ([解答を表示する](#))

最新問題: 108

COVID-19 またはその他の診断されたウイルスに関連して接触追跡アプリを設計する場合、次のプライバシー対策をすべて考慮する必要がありますが、次の項目は除きます。

- A. データの保持。
- B. 使用制限。
- C. オプトアウトの選択。
- D. ユーザーの機密性。

Answer: C ([メッセージを残す](#))

接触追跡アプリは、感染者と濃厚接触したユーザーに通知することで、公衆衛生当局が COVID-19やその他の診断されたウイルスの拡散を追跡し、封じ込めるのに役立つように設計されています。

しかし、これらのアプリは健康状態や位置情報などの機密性の高い個人データを収集・処理するため、プライバシーに関する懸念も生じます。そのため、接触追跡アプリは設計とデフォルトによるプライバシーの原則に従う必要があります。つまり、開発と運用にプライバシー対策を組み込み、ユーザーに最高レベルのプライバシー保護を提供する必要があります。接触追跡アプリを設計する際に考慮すべきプライバシー対策には次のようなものがあります。

* データ保持: 接触追跡アプリは、収集した個人データを公衆衛生目的を達成するために必要な期間のみ保持し、その後はデータを削除するか匿名化する必要があります。データ保持期間は、科学的証拠と法的要件に基づいてユーザーに明確に伝えられる必要があります。

* 使用制限: 接触追跡アプリは、収集した個人データを接触追跡という特定の正当な目的にのみ使用し、商業、法執行、監視などの他の目的に使用してはなりません。使用制限は、暗号化、アクセス制御、監査などの技術的および組織的な手段によって実施する必要があります。

* ユーザーの機密性: 接触追跡アプリは、ユーザーの個人データと身元の機密性を保護し、ユーザーの同意または法的許可なしに第三者に開示してはなりません。ユーザーの機密性は、仮名化、集約、データ最小化などの技術的および組織的な対策によって確保する必要があります。

一方、オプトアウトの選択は、接触追跡アプリの有効性と公衆衛生の目的を損なうため、接触追跡アプリを設計する際に考慮すべきプライバシー対策ではありません。接触追跡アプリが適切に機能し、目的を達成するには、ユーザーの自発的な参加と広範な採用が必要です。

したがって、ユーザーにアプリや、データ共有や通知などの特定の機能からオプトアウトするオプションを提供すると、アプリの対象範囲と精度が低下し、ユーザーや他の人をより大きな健康リスクにさらす可能性があります。オプトアウトの選択肢の代わりに、接触追跡アプリは、アプリの仕組み、収集するデータとその使用方法、アプリがもたらすメリットとリスク、ユーザーがデータに対して持つ権利と管理権について、明確で透明性のある情報をユーザーに提供する必要があります。これにより、ユーザーは自分の好みや価値観に基づいて、十分な情報に基づいて自発的にアプリを使用するかどうかを決定できます。

参考文献:

* [IAPP CIPP/US 学習ガイド]、第 2 章: プライバシーバイ デザインとデフォルト、35-36 ページ。

* [IAPP CIPP/US Body of Knowledge]、セクション II: 民間部門によるデータの収集と使用の制限、サブセクション B: プライバシーバイ デザイン、9-10 ページ。

* [IAPP 用語集]、用語: 接触追跡、プライバシーバイ デザイン、プライバシーバイ デフォルト。

2012年のオバマ政権の報告書で提示された「消費者プライバシー権利章典」は、一般的に何に基づいていますか？

- A. 1974年プライバシー法
- B. コモンローの原則
- C. 欧州連合指令
- D. 伝統的な公正な情報慣行

Answer: [\(解答を表示する\)](#)

2012年のホワイトハウスレポートには、オバマ大統領が署名した序文が含まれており、従来の公正情報慣行 (FIP) に基づいて「消費者プライバシー権利章典」が定義されています。」

最新問題: 110

「電子情報開示」の規則は主に次のどれを防止しますか？

- A. ビジネス慣行と技術的安全対策の矛盾
- B. 不適切なデータ保持方法による情報の損失
- C. 従業員が個人所有のデバイスを仕事に利用する慣行
- D. 組織のデータ保持プログラムの違反

Answer: B ([メッセージを残す](#))

学習教材の 346 ページ - 「.....電子証拠開示規則では、裁判前の証拠開示手続き中に、電子メールやその他の企業文書を自動化して大量に作成することが義務付けられています」。

最新問題: 111

シナリオ

次の質問に回答するには、以下を使用してください。

ラリーは、サンライズリンクスでのテレマーケティングの職務、特に上司のエヴァンにますます不満を募らせている。先週、エヴァンが州の Do Not Call リストとそこに載っている人々をあざ笑っているのを耳にした。迷惑をかけたくないと本気で思っているなら、全国 DNC リストに載っているはずだ。それが私たちが従わなければならない唯一のリストだ。サンライズリンクスでは、電話しないでほしいと言われるまで電話をかけ続ける」。奇妙なことに、エヴァンはテレマーケティング担当者に、受信者が「別の機会に」電話してほしいと頼んだ場合の記録を残すよう要求している。ラリーにとって、これは彼らがまったく電話を受けたくないという明らかな兆候だ。エヴァンはそうは考えていない。

ラリーは、エヴァンの傲慢さが従業員への接し方にも影響していると考えています。米国憲法は米国の労働者を保護しており、ラリーはサンライズリンクスの従業員の権利が定期的に侵害されていると考えています。最初、エヴァンはソーシャルメディアで従業員と交流するなど、友好的に見えました。しかし、エヴァンの政治的な投稿の後、ラリーは、昇進を申し出られるのは同様の所属を持つ従業員だけであることに気づきました。

さらに、ラリーは時々、私的使用の品が入った小包を職場に郵送してもらっています。名前がはっきり記されているにもかかわらず、すでに開封された状態で届いたことが何度かありま

した。ラリーは、サンライズリンクスでは私的郵便物の開封は一般的であり、エヴァンのリーダーシップの下では憲法修正第4条の権利が踏みにじられていると考えています。

ラリーは同僚のセイディーに関する会話を耳にして落胆したこともある。テレマーケティングの電話は品質保証のために定期的に録音されており、セイディーは仕事中は常にプロフェッショナルだが、私的な会話には性的な発言が含まれることがある。ラリーはエヴァンがこれについても笑っているのを聞いたことがある。彼が同僚にこのことを話すと、彼の懸念は肩をすくめるだけで済んだ。同僚は、従業員は入社時に監視されることに同意していると思っていた。個人のデバイスには手を付けていないが、電話、メール、閲覧履歴はすべて監視対象となっている。実際、ラリーは、外部の会社による覆面調査で不正行為の証拠が見つかり、従業員が解雇された事例を1件知っている。その従業員は会社から盗んだのかもしれないが、エヴァンは何かおかしいと最初に疑った時点で当局に連絡すればよかったのだ。ラリーは行動を起こしたいと思っていますが、どのように進めればよいかわかりません。テレマーケティングの実践に関して、スーパーバイザーのエヴァンは次のような誤解を抱いています。

- A. コールバックを希望する受信者の希望
- B. 受信者がオプトアウトできる条件
- C. 州法と連邦法の関係
- D. 品質保証のための監視権

Answer: ([解答を表示する](#))

最新問題: 112

組織が、高機密性として分類されたデータを低機密性として分類されたデータと同じシステムで保持する場合、最も起こり得る結果はどれですか？

- A. 組織は、ほとんどの業界固有のプライバシーおよびセキュリティ法に準拠し続けます。
- B. 組織のデータ侵害の影響は、データが分離されていた場合よりも深刻になります。
- C. 臨時従業員は、職務を遂行するために必要なデータを見つけることができます。
- D. 組織は、必要以上の情報を提出することなく、法的証拠開示要求に効率的に対応できるようになります。

Answer: B ([メッセージを残す](#))

「すべてのデータを1つのシステムに保存すると、単一の侵害による影響が拡大する可能性があります」抜粋: 「APP_US_TB_US-Private-Sector-Privacy-3E_1.0」。Apple Books。

最新問題: 113

シナリオ

次の質問に回答するには、以下を使用してください。

ある晩、マットは息子の寝室に行って、息子がベッドに寝そべってノートパソコンを打っているのを見つけた。ネットワークの調子はいかが？」とマットは期待を込めて尋ねた。

「いいえ」少年は言った。アンケートに答えているところです。」

マットは息子の肩越しに自分のコンピューターの画面を見た。『どんな調査?』私の意見についての質問だよ。」

「ちょっと見てみよう」とマットは言い、息子がすでに答えた質問のリストを読み始めた。政府と市民権についての意見を聞いているんだ。ちょっと変だな。君はまだ10歳なのに。」マットは、どうしてこのアンケートのウェblinkが息子のメールの受信箱に入ってしまったのか不思議に思った。このメッセージは息子に間違って送られたのかもしれないと思い、開いて読んでみた。このメッセージは、リーダーシップ プロジェクトという団体から送られてきたもので、内容と画像から子供向けであることがわかった。マットが読み進めると、アンケートに答えた子供は自動的に、有名なリーダーに関するシリーズの最初の本が当たるコンテストに登録されることがわかった。

マットにとって、これは明らかに子供たちに商品やサービスを売り込むためのマーケティング戦略に思えました。彼は息子に、アンケートに答えるために自分自身の情報を提供するよう求められたかどうか尋ねました。息子は、名前、住所、電話番号、生年月日を尋ねられ、好きなゲームやおもちゃについての質問に答えるよう求められたと答えました。

マットは心配していました。マーケティング担当者が息子からこのような方法で情報を収集することが合法かどうか疑問に思いました。その後、息子の受信箱に子供向けの商品を宣伝するマーケティング担当者からの他のいくつかの商業メールが届いていることに気づき、この事件を適切な当局に報告する時だと判断しました。

この事件を踏まえると、FTCによるマーケティング担当者に対する強制措置にはどのような違反が含まれる可能性が高いでしょうか?

- A. 13歳未満の子供から情報を収集します。
- B. 小さな子供がいる家族のプライバシーを侵害する。
- C. 子供向けマーケティング業界のプライバシーポリシーを無視しています。
- D. 児童の個人情報の漏洩を通知しなかった。

Answer: C (メッセージを残す)

最新問題: 114

ビデオゲームのデジタル キーを販売するオンラインストアであるあなたの会社は、ある個人からデータ アクセス要求を受け取りました。具体的には、その個人は先月購入した複数のゲームのデジタル キーを含むメールを紛失したため、最近の購入履歴にアクセスしたいと考えています。

セキュリティの観点から、CCPAに基づいてユーザーが自分の身元を適切に確認するためには、何を行う必要がありますか?

- A. 運転免許証と一緒に自分の写真を撮る
- B. 2人の証人が署名した公証済みの宣誓供述書を提出してください。
- C. 会社のパスワード保護されたアカウントにログインする
- D. 会社に電話して連絡先とクレジットカード番号を伝える

Answer: C (メッセージを残す)

カリフォルニア州消費者プライバシー法 (CCPA) に基づき、企業は個人情報のセキュリティを確保するために、データ アクセス要求を行う個人の身元を確認する必要があります。消費者の身元を確認する最も安全で簡単な方法は、個人にパスワードで保護されたアカウントにログインするよう要求することです。これにより、要求者がアカウント所有者であることが証明されます。

パスワードで保護されたアカウントが検証に最適な理由:

* アカウントベースの関係: 消費者が企業にパスワードで保護されたアカウントを持っている場合、通常は消費者にそのアカウントにログインしてもらうことで検証できます。これは、CCPA ガイドラインに基づく十分な本人確認方法と見なされています。

* リスクの最小化: アカウントログインを通じて本人確認を行うと、ログイン資格情報にアクセスできるのはアカウント所有者のみとなるため、個人情報への不正アクセスのリスクが軽減されます。

オプションの説明:

* A. 運転免許証と一緒に自分の写真を撮る: これは本人確認にはなりませんが、より侵入的であり、個人情報盗難の不必要なリスクをもたらします。これは、CCPA では推奨される方法でも一般的な方法でもありません。

* B. 2人の証人が署名した公証済みの宣誓供述書を提供する: これはほとんどの場合、特にオンラインストアの場合、本人確認には過剰であり非現実的です。

* C. 会社のパスワードで保護されたアカウントにログインする: 正解です。パスワードで保護されたアカウントにログインすることは、CCPA に基づいてリクエスト者の身元を確認する簡単で安全な方法です。

* D. 会社に電話して連絡先とクレジットカード番号を伝える: この方法は安全ではありません。第三者がこの情報を提供すると、個人情報の盗難や不正アクセスにつながる可能性があります。

CIPP/US 資料からの参照:

* CCPA 規則 (11 CCR § 999.323): パスワードで保護されたアカウントの使用を含む、本人確認の要件を指定します。

* IAPP CIPP/US 認定テキスト: CCPA に基づいて消費者の身元を確認するための安全な方法について説明します。

最新問題: 115

ほとんどの州法の下で、組織が違反通知要件の対象となるために一般的に要求されるのは次のどれですか?

- A. エンティティは州内に従業員を保有している必要があります
- B. 当該事業体は州内で事業を行う必要がある
- C. エンティティは情報ブローカーである必要があります
- D. エンティティは州に登録されている必要があります

Answer: B ([メッセージを残す](#))

最新問題: 116

グラム・リーチ・ブライリー法 (GLBA) が個人の銀行口座への不正アクセスを防止する主な方法は何ですか？

- A. セキュリティ侵害の疑いがある場合、直ちに公表を要求する。
- B. 顧客の個人情報を紙に印刷することを義務付けます。
- C. 金融機関に個人情報の収集を制限するよう要求する。
- D. 金融機関による顧客口座番号の開示を制限することにより。

Answer: D (メッセージを残す)

GLBA は、金融機関が消費者の口座番号または同様のアクセス番号やアクセスコードを、テレマーケティング、ダイレクトメールマーケティング、または電子メールによる消費者へのその他のマーケティングに使用するために、関連会社ではない第三者に開示することを禁止しています。この制限は、口座番号を使用して不正な取引や個人情報の盗難を開始する可能性のある第三者による個人の銀行口座への不正アクセスを防止することを目的としています。GLBA はまた、金融機関に対して、顧客情報のセキュリティ、機密性、および整合性を保護するための安全策を実装し、そのような情報に関連するセキュリティ侵害が発生した場合に顧客と規制当局に通知することを義務付けています。参考資料:

* IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第 2 章: 民間部門によるデータの収集と使用の制限、セクション 2.3: 金融プライバシー、p. 49-50

* IAPP CIPP/US 知識体系、ドメイン II: 民間部門によるデータの収集と使用の制限、目標 II.C: 金融機関のプライバシー要件を特定する、サブ目標 II.C.2: 口座番号の開示に関する制限を特定する、p. 14

* IAPP CIPP/US 試験ブループリント、ドメイン II: 民間部門によるデータの収集と使用の制限、目標 II.C: 金融機関のプライバシー要件を特定する、サブ目標 II.C.2: 口座番号の開示に関する制限を特定する、p. 5

最新問題: 117

2012 年に、ホワイトハウスと FTC は両方とも、プライバシーの施行に対する新しいアプローチを提唱するレポートを発行しましたが、そのアプローチを最もよく表すものは何ですか。

- A. 危害ベース。
- B. 自己規制。
- C. 包括的。
- D. 気づきと選択。

Answer: C (メッセージを残す)

2012 年、ホワイトハウスは「ネットワーク化された世界における消費者データ プライバシー: グローバル デジタル エコノミーにおけるプライバシーの保護とイノベーションの促進のためのフレームワーク」と題するレポートを発表し、公正情報慣行原則 (FIPP) に基づく消費者プライバシー権利章典を提案しました。このレポートでは、関連するテクノロジーやビジネス モデルに関係なく、すべての商業セクターとすべての個人データに適用される包括的なプライバシー フレームワークを求めました。また、このレポートでは、議会にこのフ

フレームワークを実装するための法律を制定し、FTC にそれを施行する権限を与えるよう求めました。同様に、FTC は「急速な変化の時代における消費者プライバシーの保護: 企業と政策立案者への推奨事項」と題するレポートを発表し、企業が消費者のプライバシーを保護し、イノベーションを促進するための一連のベスト プラクティスを概説しました。このレポートでは、オンラインとオフラインの両方のデータをカバーし、特定の消費者、コンピューター、またはデバイスに合理的にリンクできる消費者データを収集または使用するすべてのエンティティに適用される包括的なプライバシー フレームワークも提唱しました。また、このレポートでは、議会が基本プライバシー法を制定し、FTC にそれを実装するための規則制定権限を与えることを検討するよう勧告しました。したがって、両報告書は、被害に基づく、自主規制、または通知と選択のアプローチではなく、プライバシーの施行に対する包括的なアプローチを提唱していると言えます。参考文献: ホワイトハウス報告書、FTC 報告書、IAPP CIPP/US 学習ガイド (31-32 ページ)

最新問題: 118

シナリオ

次の質問に答えるには、以下を使用してください。

デクランさんはウッドランド病院の放射線科で看護助手として働き始めたばかりです。また、正看護師になるためのプログラムも始めました。

このキャリアに進む前、デクランは医療保険の携行性と責任に関する法律 (HIPAA) について漠然と知っていました。彼は現在、患者の保護対象医療情報 (PHI) のセキュリティを確保するために尽力する必要があることを認識しており、プライバシーの問題について慎重に考えています。

初日の朝、デクランは、新しく雇われた受付係が各患者に HIPAA プライバシー通知を渡していることに気づきました。彼は、再診患者にこれらのプライバシー通知を渡す必要があるかどうか、また、放射線科部門が 1 回限りの配布システムによって紙の無駄を減らせないかと考えました。

彼はまた、病院が請求会社を利用していることにも興味を持っていました。請求会社が患者の治療に関する詳細を知っている場合、病院は患者のプライバシーを保護するためにできる限りのことをしているのだろうかという疑問を呈しました。

デクランは初日に、病院の大きな放射線科のあらゆるエリアに精通しました。途中で残された機器を整理していたとき、病院の管理者 2 人の会話を耳にしました。暗号化されていない患者情報を含むポータブルハードドライブが紛失したと聞いて、デクランは驚きました。管理者は、病院が責任を回避できることに安堵しました。デクランは驚き、何が起こったのかを病院が適切に報告する計画があるかどうか疑問に思いました。

デクランはこの問題について懸念を抱いていたものの、電子医療記録 (EHR) を患者の日常的なケアに統合しようとする病院の取り組みに驚きました。全国のすべての医療施設で EHR にアクセスできれば、ケアをさらに効率化できる可能性があると考えました。

デクランは患者と多くの良い関係を築いた。初日の終わりに、彼はジョンという患者と話をした。彼の父親は変性性筋疾患と診断されたばかりだった。ジョンは血液検査を受けるとこ

ろだったが、血液検査で病気の遺伝的素因が明らかになり、保険適用を受けられなくなるのではないかと心配していた。デクランはジョンに、そんなことはあり得ないと思うと伝えたが、患者は理由を説明する前に車椅子で運び去られてしまった。ジョンはこの件について同僚に尋ねるつもりだ。

デクランは、1か月後に、自分の選んだ健康に関するトピックの授業でレポートを提出しなければなりません。それまでに、デクランは、事例として使える患者とのやり取りをたくさん経験しているでしょう。遺伝子検査についてもっと慎重に考えるきっかけを与えてくれたジョンに、デクランは名前を挙げて感謝の意を表すでしょう。

デクランの一日は多くの質問で終わりましたが、彼は新しい役職に満足していました。放射線科は、デクランの紙の無駄に関する懸念に対処しながら、医療保険の携行性と責任に関する法律 (HIPAA) に準拠するにはどうすればよいでしょうか？

- A. 患者が初回診察時にプライバシー通知を受け取っていることを確認する
- B. 代わりに目立つ場所にプライバシー通知を掲載する
- C. 患者を病院のウェブサイトの適切なエリアに誘導する
- D. 患者にプライバシーポリシーを口頭で伝える

Answer: C (メッセージを残す)

最新問題: 119

カリフォルニア州消費者プライバシー法 (カリフォルニア州プライバシー権利法による改正後)に基づき、消費者は企業に対して民事訴訟を起こすことができますか？

- A. 不正アクセスや漏洩の対象となる個人情報。
- B. 暗号化も編集もされていない特定の個人情報のセキュリティ侵害
- C. 保有する個人情報を保護するために、合理的なセキュリティ手順と実践を実施および維持していない。
- D. カリフォルニア州プライバシー保護局 (CPPA) が発行した規制に定められたセキュリティ対策を実装および維持していない。

Answer: B (メッセージを残す)

カリフォルニア州消費者プライバシー法 (CCPA) は、カリフォルニア州プライバシー権利法 (CPRA) によって改正され、企業が消費者の個人情報を適切に保護せず、セキュリティ侵害が発生した場合に、消費者は民事訴訟を起こす権利を有します。この権利は、暗号化も編集もされていない特定のカテゴリの個人情報の侵害に特に適用されます。

CCPA/CPRA 民事訴訟の主な詳細:

* セキュリティ侵害:

* 漏洩に社会保障番号、運転免許証番号、金融口座情報などの個人情報が関係する場合、データが暗号化されておらず、編集されていない限り、消費者は企業を訴えることができます。

* 合理的なセキュリティ対策:

* 企業は、個人情報を保護するために、合理的なセキュリティ対策を実施し、維持する必要があります。これを怠ると、違反が発生した場合に企業が責任を問われる可能性があります。

* 対象となるデータのカテゴリ:

* 法律では、特定の機密カテゴリの個人情報のみが民事訴訟の対象となることが規定されています。

オプションの説明:

* A. 不正アクセスや漏洩の恐れのある個人情報 :これは誤りです。

民事訴訟はすべての個人情報ではなく、特定の機密データカテゴリに限定されます。

* B. 暗号化も編集もされていない特定のカテゴリの個人情報のセキュリティ侵害:これは正解です。CCPA/CPRA に基づく民事訴訟は、暗号化も編集もされていない特定の機密データに関する侵害に適用されます。

* C. 保有する個人情報を保護するための合理的なセキュリティ手順と慣行を実施および維持していないこと:これは法律上の要件ですが、それだけでは民事訴訟の根拠にはなりません。消費者が訴訟を起こすには、セキュリティ侵害が発生している必要があります。

* D. カリフォルニア州プライバシー保護局 (CPPA) が発行した規制に定められたセキュリティ対策を実施および維持していない:これは誤りです。民事訴訟は機密データの漏洩に関連しており、特定の機関のガイドラインを満たしていないこととは関係ありません。

CIPP/US 資料からの参照:

* CCPA/CPRA (民法 § 1798.150): 暗号化および編集されていない特定のデータに関連するセキュリティ侵害に対する民事訴訟権の概要を示します。

* IAPP CIPP/US 認定テキスト: 消費者が CCPA/CPRA に基づいて民事訴訟を起こすことができる条件について説明します。

最新問題: 120

次の連邦機関のうち、公正かつ正確な信用取引法 (FACTA) に基づく廃棄規則を施行しないのはどれですか?

- A. 通貨監督庁
- B. 消費者金融保護局
- C. 保健福祉省
- D. 連邦取引委員会

Answer: ([解答を表示する](#))

* 公正かつ正確な信用取引法 (FACTA) に基づく廃棄規則は、消費者レポートから得られた消費者情報を保持または保有する個人または団体に対し、その情報を安全かつ適切な方法で廃棄することを要求する連邦規制です¹。

* 廃棄規則は、個人情報への不正アクセスや不正使用を防止することにより、個人情報の盗難や詐欺から消費者を保護することを目的としています¹。

* 廃棄規則は、規則の対象となる事業体の種類と部門に応じて、複数の連邦機関によって施行されます¹。これらの機関には以下が含まれます。

* 連邦取引委員会 (FTC) は、他の機関によって具体的に規制されていないほとんどの団体に対して一般的な権限を持っています²。

* 消費者金融保護局 (CFPB) は、銀行、信用組合、貸金業者、債権回収業者、信用調査機関などの消費者金融商品およびサービスに対する権限を有します³。

* 通貨監督庁 (OCC)。国立銀行および連邦貯蓄協会に対して権限を有します⁴。

- * 連邦預金保険公社 (FDIC)。連邦準備制度に加盟していない州認可銀行および州認可貯蓄協会5に対して権限を有します。
- * 連邦準備制度理事会 (FRB)は、連邦準備制度に加盟している州認可銀行、銀行持株会社、および銀行持株会社の特定の非銀行子会社に対して権限を有します。
- * 連邦政府が保証する信用組合に対して権限を持つ全米信用組合管理局 (NCUA)。
- * 証券取引委員会 (SEC)。ブローカー、ディーラー、投資会社、投資顧問に対して権限を有します。
- * 商品先物取引委員会 (CFTC)。商品先物およびオプション市場と仲介業者に対する権限を有します。
- * 保健福祉省 (HHS) は、FACTA に基づく廃棄規則を施行する連邦機関の 1 つではありません。HHS は、医療保険の携行性と責任に関する法律 (HIPAA) および経済的および臨床的健全性のための医療情報技術に関する法律 (HITECH) に基づいて医療情報のプライバシーとセキュリティに関する権限を有していますが、FACTA に基づいては権限を有していません。参照: 1: 消費者レポート情報を廃棄する? ルールでその方法が説明されています 2: FTC の執行 3: CFPB の執行 4: OCC の執行 5: FDIC の執行: [FRB の執行]: [NCUA の執行]: [SEC の執行]: [CFTC の執行]: [HHS の執行]

最新問題: 121

シナリオ

次の質問に回答するには、以下を使用してください。

シェリルは、Fitness Coach, Inc. の唯一の所有者です。同社は、クラス、個人指導、大規模な屋内ジムへのアクセスを通じて、個人のフィットネス目標の実現を支援する中規模企業です。彼女は 10 年間この会社を経営しており、常に最高レベルのサービスを維持しながら顧客のプライバシーを保護することに配慮してきました。彼女は、顧客と長期にわたる関係を築いてきたことを誇りに思っています。

シェリルとスタッフはプライバシー保護を最優先にしようと努めてきましたが、会社には正式なプライバシーポリシーがありませんでした。そこでシェリルはプライバシーの専門家であるジャニスを雇い、ポリシーの作成を手伝ってもらいました。

最初の評価の後、ジャニスは新しいポリシーの最初のものを作成しました。シェリルは草案を読み、このポリシーが会社全体にもたらす多くの変更を懸念しました。たとえば、草案では、パーソナルトレーナーとのセッションなどのサービスに対して顧客の個人情報を支払った後、1年間のみ保持できると規定されています。また、顧客の書面による同意なしに顧客情報を第三者と共有しないことも約束しています。これらの規則の文言はシェリルを心配させます。なぜなら、保存された個人情報は、顧客が長い間訪問していなくても、会社が顧客にサービスを提供するのに役立つことが多いからです。さらに、契約ベースでクラスを教えるエアロビクスのインストラクターなど、重要なサービスを提供するサードパーティもいます。顧客ファイルにアクセスし、生徒のフィットネスレベルを理解することは、インストラクターがクラスを編成するのに役立ちます。

ジャニスはシェリルの懸念を理解し、すでにいくつかの修正案を練っていました。顧客データは保持できるが、機密性のレベルに応じて分類する必要があることを指摘して、シェリルを安心させようとしていました。しかし、シェリルは懐疑的でした。データを分類し、タイプごとに異なる取り扱いをすると、会社の日常業務に不必要な困難が生じるように思われました。シェリルは、必要に応じてすべての従業員がアクセスできる、1つのシンプルなデータストレージおよびアクセスシステムを望んでいます。

プライバシーポリシーはまだ草案に過ぎませんでした。彼女は社内に変更が必要になるだろうと感じ始めていました。彼女はジャニスに、数か月かけて1部門ずつ新しいポリシーを徐々に導入する方が安心できるだろうと伝えました。また、新しいポリシーの適用可能な部分を各部門にリストしたドキュメントを作成するという階層化アプローチにも興味がありました。

シェリルが提案した新しいプライバシーポリシーの伝達方法の主な問題点は何ですか？

- A. 従業員は、時間をかけて実行されるポリシーに満足しないでしょう。
- B. ポリシーは、完全に伝達されなければ有効とはみなされません。
- C. 従業員は、文書がポリシー全体とどのように関連しているかを理解していない可能性があります。
- D. ポリシーは部門間で一貫して実装されない可能性があります。

Answer: ([解答を表示する](#))

有効な **CIPP-US** 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集！ GoShiken.com が最新の **CIPP-US** 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (**22830%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 122

次のどれが、HIPAA プライバシー ルールに基づく承認要件の例外に該当しないでしょうか。

- A. 医療上の緊急事態を治療するために必要な健康情報を開示します。
- B. 公衆衛生活動のために健康情報を公開します。
- C. 児童虐待の報告を提出するために健康情報を開示する。
- D. サードパーティの請求管理者に支払うために必要な健康情報を開示します。

Answer: A ([メッセージを残す](#))

最新問題: 123

次のすべての慣習法上の不法行為は、米国法の下では従業員のプライバシーに関連しますが、次の例外はありません。

- A. 精神的苦痛を与えること。

- B. 変換。
- C. 名誉毀損
- D. 隔離への侵入。

Answer: B (メッセージを残す)

最新問題: 124

スミス メモリアル ヘルスケア (SMH) は、ニューヨークに本社を置き、他の 7 州で事業を展開している病院ネットワークです。SMH は電子医療記録を使用して患者に関する情報を入力し、追跡しています。最近、SMH はデータ侵害に遭い、第三者のハッカーが SMH の内部ネットワークにアクセスできました。

SMHはHIPPAの対象となる事業体であるため、米国公民権局に通知を行った。

侵害について保健福祉省に報告した。

SMH の通知責任を正確に説明している記述はどれですか？

- A. SMH が HIPAA に準拠している場合、ニューヨーク州の個人に対して個別の通知を行う必要はありません。
- B. SMH がニューヨーク州で 500 人を超える患者を抱えている場合、これらの患者に対して個別の通知を行う必要があります。
- C. SMH が事業を展開している他の州で通知を行う必要がある場合は、ニューヨーク州の個人にも通知を行う必要があります。
- D. SMH が問い合わせる個人に対して信用監視を提供する場合、ニューヨーク州の個人に対して別途通知する必要はありません。

Answer: C (メッセージを残す)

正解は C です。SMH が事業を展開している他の州で通知する必要がある場合、ニューヨーク州の個人にも通知する必要があります。医療保険の携行性と責任に関する法律 (HIPAA) に基づき、SMH は、保護されていない保護対象医療情報 (PHI) に関するデータ侵害を発見後 60 日以内に、公民権局 (OCR) と影響を受ける個人に通知する必要があります¹。ただし、HIPAA は、個人に強力な保護を提供したり、対象事業体に追加の義務を課したりする州法に優先するものではありません²。したがって、SMH は、ニューヨーク州を含む事業を展開している州の州法違反通知法にも準拠する必要があります。

ニューヨーク州情報セキュリティ侵害および通知法によれば、ニューヨーク州居住者の個人情報を含むコンピュータ化されたデータを所有またはライセンス供与する個人または企業は、個人情報の漏洩が不注意によるものであり、悪用または金銭的損害につながる可能性が低い場合を除き、システムのセキュリティ侵害を可能な限り速やかに、不当に遅延することなく当該居住者に開示する必要があります³。個人情報には、個人情報（名前、番号、またはその他の識別子など）に加えて、社会保障番号、運転免許証番号または非運転者身分証明書番号、口座番号、クレジットカードまたはデビットカード番号と、個人の金融口座へのアクセスを許可する必要なセキュリティコード、アクセスコード、パスワード、またはその他の情報との組み合わせ、生体認証情報、またはユーザー名または電子メールアドレスと、オンラインア

カウントへのアクセスを許可するパスワードまたはセキュリティの質問と答えとの組み合わせが含まれます3。

したがって、SMH のデータ侵害がニューヨーク州住民のこれらのデータ要素のいずれかに関係する場合、SMH が HIPAA に準拠しているかどうか、ニューヨーク州に 500 人以上の患者がいるかどうか、または信用監視サービスを提供しているかどうかに関係なく、SMH は侵害について彼らに通知する必要があります。また、SMH は影響を受けた個人に通知してから 10 日以内にニューヨーク州司法長官、国務省、州警察局に通知する必要があります3。さらに、侵害が電子医療記録に関係する場合、SMH はニューヨーク州保健局に通知する必要があります4。

参考資料: <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-on-Managing-and-Notifying-Data-Breaches-under-the-PDPA-15-Mar-2021.pdf?la=en>

https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_note_dbn_e.pdf

最新問題: 125

グラム・リーチ・ブライリー法 (GLBA) に基づいて銀行は何をする必要がありますか?

- A. ユーザーの嗜好に対する満足度に関する消費者調査を毎年実施する
- B. 指定された時間枠内でユーザー設定の変更要求を処理する
- C. 消費者にテレマーケティングの電話を受け取らないよう選択する機会を提供する
- D. 個人情報 を提携関係のない第三者に譲渡して第三者自身の使用に供する前に、オプトアウトを提案する

Answer: (解答を表示する)

グラム・リーチ・ブライリー法 (GLBA) は、銀行、信用組合、証券会社、保険会社などの金融機関が収集、使用、開示する消費者金融情報のプライバシーとセキュリティを規制する連邦法です12。GLBA に基づき、金融機関は、プライバシー ルールとセーフガード ルール12 という 2 つの主要なルールを遵守する必要があります。プライバシー ルールでは、金融機関が顧客に情報共有慣行について通知し、子供から個人情報を収集、使用、開示する前に検証可能な親の同意を得ることが義務付けられています12。プライバシー ルールでは、例外が適用されない限り、顧客に個人情報が特定の非関連第三者と共有されることを拒否する権利も与えられています12。セーフガード ルールでは、金融機関が顧客情報の機密性、セキュリティ、整合性を保護する包括的な情報セキュリティ プログラムを開発、実装、維持することが義務付けられています12。

したがって、銀行やその他の金融機関は、顧客が要求または承認した取引を完了するために開示が必要な場合や、情報を保護し、開示された目的にのみ使用することに同意したサービスプロバイダーまたは共同マーケティング担当者に開示する場合など、例外が適用されない限り、個人情報 (PI) を関連のない第三者に転送して第三者が独自に使用する前にオプトアウトを提供する必要があります12。この要件は、金融機関による個人情報の使用と共有方法を顧客がより細かく制御できるようにし、顧客のプライバシー権を保護することを目的としています12。

参照: 1: グラム・リーチ・ブライリー法 | 連邦取引委員会、1. 2: グラム・リーチ・ブライリー法の消費者金融情報のプライバシー規則に準拠する方法 | 連邦取引委員会、2.

最新問題: 126

公正信用報告法 (FCRA) と公正かつ正確な信用取引法 (FACTA) の規則制定権限を持つのは誰ですか？

- A. 州司法長官
- B. 連邦取引委員会
- C. 商務省
- D. 消費者金融保護局

Answer: D (メッセージを残す)

消費者金融保護局 (CFPB) は、公正信用報告法 (FCRA) および公正かつ正確な信用取引法 (FACTA)、ならびにその他の消費者金融法の規則制定権限を有しています。2010 年に制定されたドッド・フランク法は、FACTA およびクレジットカード法によって FCRA に追加された規則制定責任のほとんどを連邦取引委員会 (FTC) から CFPB に移管しました。ただし、FTC は、他の連邦および州機関とともに、FCRA および FACTA の執行権限を保持しています¹。CFPB は、個人情報盗難の危険信号や住所不一致ルールなど、FACTA の一部の規定の規則制定権限を FTC と共有しています²。商務省および州司法長官は、FCRA または FACTA の規則制定権限を持っていません。参照: 1: FTC³、公正信用報告法⁴: CFPB。

最新問題: 127

シナリオ

次の質問に回答するには以下を使用してください

大手小売店で顧客の個人情報と財務情報を含むデータ侵害が発生したとき、会社の役員たちは衝撃を受けました。しかし、同社のプライバシーアナリストであり、自身も個人情報盗難の被害者であるロベルタは衝撃を受けませんでした。侵害が発生する前、彼女は役員向けのプライバシープログラムレポートに取り組んでいました。会社が組織全体でデータを共有し、処理する方法が大きな懸念事項でした。顧客情報へのアクセスに関する適切なルールも、古くなったデータを消去および破棄する手順もありませんでした。ロベルタは調査の中で、下級従業員でさえ会社のすべての顧客データ (財務記録を含む) にアクセスでき、1980 年代にさかのぼる古い顧客データがまだ会社に残っていることを発見しました。

彼女の報告書では、3つの主要な改革を推奨しています。まず、必要に応じてアクセスを許可すること。つまり、従業員が顧客情報にアクセスできるのは、業務に関連するデータのみ制限するということです。次に、顧客の財務情報 (クレジットカード番号や銀行口座番号など) を機密性の低い情報とは別に保管するための、非常に安全なデータベースを作成します。最後に、古くなった顧客情報を特定し、安全に廃棄するプロセスを作成します。

侵害が発生したとき、同社の幹部はロベルタを会議に招集し、彼女は報告書で推奨事項を提示しました。ロベルタは、同社が全国規模の顧客基盤を持つということは、関連するすべての州の侵害通知法に準拠する必要があることを説明しました。ロベルタの指導のおかげで、同

社は州の侵害通知法で定められた特定の時間枠内で迅速に顧客に通知することができました。

その後すぐに、役員らはロベルタが報告書で推奨したプライバシー プログラムの変更を承認しました。これらの変更により、またプライバシーとセキュリティがすべての従業員の責任とみなされるようになったことにより、プライバシー プログラムははるかに効果的になりました。

ロベルタが指摘した同社のプライバシー セキュリティの問題に基づくと、侵害の最も可能性の高い原因は何でしょうか？

- A. 第三者と共有された情報の意図しない開示。
- B. アクセス制御の欠如による情報の不適切な取り扱い。
- C. POS端末でのクレジットカード盗難を伴う詐欺。
- D. コンピューターやフラッシュドライブなどの会社の資産を紛失しました。

Answer: B ([メッセージを残す](#))

最新問題: 128

より厳しい州法を優先する規定を含まない連邦法はどれですか？

- A. CAN-SPAM法
- B. 児童オンラインプライバシー保護法 (COPPA)
- C. 公正かつ正確な信用取引法 (FACTA)
- D. 電話勧誘消費者保護および詐欺防止法

Answer: ([解答を表示する](#))

より厳しい州法を優先する規定を含まない連邦法は、テレマーケティング消費者保護および詐欺防止法¹です。この法律は、連邦取引委員会 (FTC) に、電話禁止登録、ロボコールの禁止、重要情報の開示などのテレマーケティング慣行に関する規則を制定および施行する権限を与えています²。ただし、この法律は、「テレマーケティング慣行に関する州法が本条の規定と矛盾する場合を除き、また矛盾する範囲でのみ、本条の規定の対象となる人物を無効、変更、または影響を及ぼしたり、遵守を免除したりするものではない」とも明確に述べています¹。これは、州が連邦法よりも保護が劣らない限り、テレマーケティングに関する独自の法律を制定および施行できることを意味します。対照的に、質問に挙げられている他の3つの法律には、電子通信、オンライン プライバシー、およびクレジット取引の特定の側面を規制する州の権限を制限または無効にする優先条項が含まれています^{3,4,5}。参照: 1: テレマーケティング消費者保護および詐欺防止法²: テレマーケティング販売規則 | 連邦取引委員会³: CAN-SPAM 法: ビジネス向けコンプライアンス ガイド⁴: 児童オンライン プライバシー保護規則 ("COPPA") | 連邦取引委員会⁵: 2003 年公正かつ正確なクレジット取引法 - Wikipedia: IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第 5 章: 連邦取引委員会と消費者プライバシー、p. 144-145、149-150、154-155

最新問題: 129

1986 年の電子通信プライバシー法による有線、口頭、電子通信の傍受禁止の例外は何ですか？

- A. 当事者の一方が同意した場合
- B. すべての当事者が同意した場合のみ
- C. 組織が従業員の個人的な通話を傍受した場合
- D. 州法がそのような傍受を許可している場合

Answer: C ([メッセージを残す](#))

最新問題: 130

法執行機関は、ACME 通信会社に対し、テロ攻撃を計画した疑いのある人物のテキストメッセージ記録へのアクセスを求める召喚状を発行しました。同社は以前、テキストメッセージ記録を暗号化し、容疑者だけがこのデータにアクセスできるようにしていました。

ACME は、法執行機関による情報へのアクセスを防ぐサービスを設計することで、どのような法律に違反したのでしょうか？

- A. SCA
- B. ECPA
- C. パス
- D. 米国自由法

Answer: ([解答を表示する](#))

ACME が法執行機関による情報へのアクセスを防ぐサービスを設計することで違反した法律は、法執行のための通信支援法 (CALEA)¹ です。CALEA は連邦法であり、通信キャリアと通信機器メーカーは、通信の傍受に関する法的要請に応じるために必要な監視機能を備えるように機器、施設、サービスを設計する必要があります²。CALEA はテキストメッセージを含むすべての商用メッセージに適用され、法執行機関にサービス プロバイダーからそのような通信の記録を召喚する権限を与えます³。ACME は、容疑者だけがこのデータにアクセスできるようにテキストメッセージの記録を暗号化することで、法執行目的での通信の傍受に協力するという CALEA の義務に違反しました。参考文献: 1: 法執行のための通信支援法 - Wikipedia²: ホーム | CALEA | 法執行機関認定委員会、Inc.³: 法執行機関向け通信支援法: IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第 6 章: 法執行機関と国家安全保障アクセス、p.

177

最新問題: 131

プライバシー ポリシーの遡及的変更に関する FTC の立場に準拠するために組織が実行できる最も重要なアクションは何ですか？

- A. ウェブサイトでポリシーの変更について説明します。
- B. 顧客から明示的な同意を得る。
- C. ソーシャルメディアを通じてポリシーの変更を公表します。
- D. 顧客の情報のセキュリティを保証します。

Answer: B ([メッセージを残す](#))

FTC は、影響を受ける消費者から積極的な同意を得ない限り、企業が以前に収集した個人情報の使用方法や共有方法に影響を与えるプライバシー ポリシーを遡及的に変更することは、

欺瞞行為であると述べています。つまり、企業は変更を明確かつ目立つように開示し、消費者の明示的な同意を得る必要があります。Web サイトでポリシーの変更を説明したり、ソーシャル メディアで宣伝したり、顧客の情報のセキュリティを保証したりするだけでは、FTC の立場に従うのに十分ではありません。参考資料:

* FTC スタッフがオンライン行動広告原則の第 3 項を改訂しました。

* プライバシーポリシーを変更するには、すべての顧客から同意を得る必要がありますか?、第 2 項。

* IAPP CIPP/US 学習ガイド、64 ページ。

最新問題: 132

グラム・リーチ・ブライリー法 (GLBA) に基づいて銀行は何をする必要がありますか?

- A. ユーザーの嗜好に対する満足度に関する消費者調査を毎年実施する
- B. 指定された時間枠内でユーザー設定の変更要求を処理する
- C. 消費者にテレマーケティングの電話を受け取らないよう選択する機会を提供する
- D. 個人情報と提携関係のない第三者に譲渡して第三者自身の使用に供する前に、オプトアウトを提供する

Answer: D ([メッセージを残す](#))

最新問題: 133

公正信用報告法 (FCRA) に基づき、信用履歴に基づいて雇用を拒否された人は何を受け取る必要がありますか?

- A. 雇用主からの迅速な通知。
- B. 雇用主に再応募する機会。
- C. 複数の消費者信用情報機関 (CRA) からの情報。
- D. 消費者金融保護局 (CFPB) からの権利のリスト。

Answer: A ([メッセージを残す](#))

FCRA では、消費者レポートの情報に基づいて応募者または従業員に対して不利な措置を講じる雇用主は、不利な措置を個人に通知しなければならないと規定されています。通知には、レポートを提供した CRA の名前、住所、電話番号、CRA が決定を下したわけではなく、不利な措置が講じられた理由を説明できないという声明、レポートの情報の正確性または完全性に異議を唱える個人の権利に関する通知、および 60 日以内に CRA からレポートの無料コピーを取得する個人の権利に関する通知を含める必要があります¹²。参考文献:

* CIPP/US 練習問題 (サンプル問題)、質問 141、回答 A、説明 A。

* IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第 4 章、セクション 4.2、p. 101-102.

* 公正信用報告法 (FCRA) 第15条、(a)項。

最新問題: 134

Global Manufacturing Co の人事部は最近、新しいソフトウェア ツールを購入しました。このツールは、メールをスキャンして候補者の発言や候補者について言われている内容を確認し、幹部候補を評価するのに役立ちます。これにより、人事部は自動化された「B60 度評価」を行えるようになり、候補者の考え方や行動、同僚や直属の部下が候補者について何を言っているか、候補者同士のやり取りがどの程度うまくいっているかを知ることができます。この新しいソフトウェアを導入する際に人事部門が行う最も重要なステップは何ですか？

- A. 従業員に、電子メールがソフトウェアによってスキャンされ、自動プロフィールが作成されることを通知します。
- B. 従業員が従業員ハンドブックを読んで署名したことを確認します。従業員ハンドブックには、EEOC によって施行される保護対象グループや法律に関係なく、組織のシステムを使用している限り、プライバシーの権利がないことが記載されています。
- C. 従業員が組織のシステムでこのソフトウェアを実行して電子メール システムをスキャンしている限り、従業員にはプライバシーの権利がないことを説明するプライバシー通知がソフトウェアに含まれていることを確認します。
- D. ソフトウェアが保護されたグループに対して意図せず差別を行わないようにします。

Answer: D (メッセージを残す)

最新問題: 135

連邦取引委員会法第 5 条の要件の対象となるベンチャーはどれですか？

- A. 地元の非営利慈善団体の募金活動
- B. オンライン販売業者の送料無料オファー
- C. 国立銀行の手数料無料当座預金プロモーション
- D. 市バスシステムの定期利用プログラム

Answer: (解答を表示する)

連邦取引委員会法 (FTC 法) 第 5 条は、商取引における、または商取引に影響を与える不正または欺瞞的な行為または慣行」を禁止しています。1 この禁止事項は、銀行を含む商取引に従事するすべての人に適用されますが、非営利団体や公共運送業者などの一部の団体は FTC の管轄から除外されます。2 したがって、4 つのオプションのうち、オンライン マーチャントの送料無料オファーのみが第 5 条の要件の対象となります。これは、消費者を誤解させたり、損害を与えたりする可能性のある商業活動に関係しているためです。たとえば、オンライン マーチャントがオファーの条件を開示しなかったり、隠れた料金を請求したり、商品を遅れてまたは破損して配送したりする場合、欺瞞的な慣行に従事することで第 5 条に違反する可能性があります。3 参考文献: 1: 第 5 条 | 連邦取引委員会 2: 連邦取引委員会法第 5 条: 不公正または欺瞞的な行為または慣行、13 ページ: IAPP CIPP/US 認定情報プライバシー 専門家学習ガイド、23 ページ。

最新問題: 136

1988 年のビデオ プライバシー保護法では、次のどれが制限されましたか？

- A. ビデオやビデオゲームの広告のターゲットとなる可能性のある人

- B. オーディオビジュアル資料の購入記録は開示される可能性があるか
{<D>}: ユーザーのオンライン動画コンテンツの視聴を監視できる場合
C. 著作権のあるオーディオビジュアル素材のダウンロードが許可されている場合
Answer: B ([メッセージを残す](#))

有効な CIPP-US 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集！ GoShiken.com が最新の CIPP-US 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (22830%OFF問題集溶と正解付きで 30%w 特別割引コード: **Freepdfdumps**)

最新問題: 137

FTC は、プライバシー原則に違反していることが判明した企業と同意判決の交渉を頻繁に行います。これは関係する両当事者にどのような利益をもたらすのでしょうか？

- A. 罰金の額を標準化します。
- B. 監査要件が簡素化されます。
- C. 潜在的に有害な宣伝を回避します。
- D. 裁判にかかる費用を節約できます。

Answer: D ([メッセージを残す](#))

同意判決とは、不公正または欺瞞的なプライバシー慣行に関与した企業と FTC との間で締結される和解契約です。同意判決では通常、企業に違法行為の停止、是正措置の実施、民事罰金の支払い、継続的な監視と報告の受け入れを求めます。同意判決は、費用がかかり、時間がかかり、不確実な裁判にかかる費用を節約できるため、関係する両当事者に利益をもたらします。また、同意判決により、裁判所に判決を課すのではなく、当事者が和解条件を交渉できるようになります。同意判決では、企業の責任や不正行為は認められませんが、法的効力があり、企業が条件に違反した場合には FTC または裁判所によって執行されます。参考文献:

- * IAPP CIPP/US 知識体系、セクション IA1.a
- * IAPP CIPP/US 教科書、第 1 章、10-11 ページ
- * FTC 同意判決

最新問題: 138

どのような状況で「消費者に選択肢を与えない」または「オプションを与えない」という政策が予想されるのでしょうか？

- A. 求職者の信用報告書が雇用主に提供される場合
- B. 顧客の住所が配送会社と共有される場合
- C. 患者の健康記録が製薬会社に提供される場合
- D. 政府から顧客の財務情報が要求された場合

Answer: B (メッセージを残す)

最新問題: 139

連邦法では、13歳未満の未成年者の個人情報を収集するための次の要件のうちどれが定められていますか？

- A. 未成年者の親または保護者からの暗黙の同意、または未成年者からの積極的な同意。
- B. 未成年者の個人情報をオンラインで収集する前に、未成年者の親または保護者の同意を得ること。
- C. 未成年者にインターネットの使用を許可する場合など、未成年者の個人情報をオンラインで収集する前に、未成年者の親または保護者からの暗黙の同意を得ること。
- D. 未成年者の個人情報をオフライン（対面など）で収集する前に、親または保護者の同意を得ること。これは、オンラインでの同意の要件も満たします。

Answer: B (メッセージを残す)

説明/参照: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0>

最新問題: 140

シナリオ

次の質問に回答するには、以下を使用してください。

デクランさんはウッドランド病院の放射線科で看護助手として働き始めたばかりです。また、正看護師になるためのプログラムも始めました。

このキャリアに進む前、デクランは医療保険の携行性と責任に関する法律 (HIPAA) について漠然と知っていました。彼は現在、患者の保護対象医療情報 (PHI) のセキュリティを確保するために尽力する必要があることを認識しており、プライバシーの問題について慎重に考えています。

初日の朝、デクランは、新しく雇われた受付係が各患者に HIPAA プライバシー通知を渡していることに気づきました。彼は、再診患者にこれらのプライバシー通知を渡す必要があるかどうか、また、放射線科部門が 1 回限りの配布システムによって紙の無駄を減らせないかと考えました。

彼はまた、病院が請求会社を利用していることにも興味を持っていました。請求会社が患者の治療に関する詳細を知っている場合、病院は患者のプライバシーを保護するためにできる限りのことをしているのだろうかという疑問を呈しました。

デクランは初日に、病院の大きな放射線科のあらゆる部分に慣れました。途中で残された機器を整理していたとき、彼は 2 人の病院管理者の会話を耳にしました。

暗号化されていない患者情報が入ったポータブルハードドライブが紛失したと聞いて、彼は驚いた。

管理者たちは、病院が責任を回避できることに安堵した。デクランは驚き、何が起こったのかを病院が適切に報告する予定があるかどうか疑問に思った。

デクランはこの問題について懸念を抱いていたものの、電子医療記録 (EHR) を患者の日常的なケアに統合しようとする病院の取り組みに驚きました。全国のすべての医療施設で EHR にアクセスできれば、ケアをさらに効率化できる可能性があると考えました。

デクランは患者と多くの良い関係を築いた。初日の終わりに、彼はジョンという患者と話をした。彼の父親は変性性筋疾患と診断されたばかりだった。ジョンは血液検査を受けるところだったが、血液検査で病気の遺伝的素因が明らかになり、保険適用を受けられなくなるのではないかと心配していた。デクランはジョンに、そんなことはあり得ないと思うと伝えたが、患者は理由を説明する前に車椅子で運び去られてしまった。ジョンはこの件について同僚に尋ねるつもりだ。

デクランは、1 か月後に、自分の選んだ健康に関するトピックの授業でレポートを提出しなければなりません。それまでに、デクランは、事例として使える患者とのやり取りをたくさん経験しているでしょう。遺伝子検査についてもっと慎重に考えるきっかけを与えてくれたジョンに、デクランは名前を挙げて感謝の意を表すでしょう。

デクランの一日は多くの質問で終わりましたが、彼は新しい役職に満足していました。放射線科は、デクランの紙の無駄に関する懸念に対処しながら、医療保険の携行性と責任に関する法律 (HIPAA) に準拠するにはどうすればよいでしょうか？

- A. 患者にプライバシーポリシーを口頭で伝える
- B. 代わりに目立つ場所にプライバシー通知を掲載する
- C. 患者を病院のウェブサイトの適切なエリアに誘導する
- D. 患者が初回診察時にプライバシー通知を受け取っていることを確認する

Answer: D (メッセージを残す)

HIPAA では、対象事業体から医療サービスを受ける個人に対して、プライバシー慣行通知 (NPP) を提供することが義務付けられています。NPP には、対象事業体が保護対象医療情報 (PHI) を使用および開示する方法、PHI に関する個人の権利、および PHI のプライバシーを保護する対象事業体の義務について記載する必要があります。NPP は、最初のサービス提供日までに、直接または電子的に個人に提供する必要があります。対象事業体は、要求に応じて NPP を提供する必要があり、Web サイトがある場合はその Web サイトに掲載する必要があります。対象事業体は、個人から NPP を受け取ったという書面による確認を得るための誠意ある努力も行う必要があります。個人が確認書への署名を拒否した場合、対象事業体はその試みと拒否の理由を文書化する必要があります。

その他のオプションは、HIPAA に準拠するには不十分です。プライバシーポリシーを口頭で伝える (オプション A) だけでは、個人が将来の参照用に保管できる NPP の書面または電子コピーは提供されません。プライバシー通知を目立つ場所に掲載する (オプション B) だけでは、個人が NPP を受け取ったり、サービスを受ける前に NPP を確認する機会が与えられることは保証されません。患者を病院の Web サイトの適切なエリアに誘導する (オプション C) だけでは、個人が NPP を電子的に受け取ることに同意し、その時点で Web サイトにアクセスしない限り、サービス提供時に個人に NPP が提供されることはありません。参考文献:

- * 保護された健康情報のプライバシー保護に関する通知
- * プライバシー保護に関するモデル通知

- * サンプル通知: プライバシー慣行に関する通知の可用性
- * プライバシー保護方針に関する通知
- * プライバシー慣行通知 (NPP) の配布と承認

最新問題: 141

カリフォルニア州在住のジョンは、年間収益 5 億ドルの大手企業でデータ侵害が発生したという通知を受け取りました。ジョンの氏名や社会保障番号など、その企業が所有していたジョンの個人情報盗まれました。ジョンはまた、その企業が彼の個人情報を保護するための適切なサイバーセキュリティ対策を講じていなかったことも知りました。

次の回答のうち、カリフォルニア州消費者プライバシー法 (CCPA) に基づいてジョンが企業に対して法的請求を追求する能力を最も正確に反映するものはどれですか？

- A. CCPA に基づいて訴訟を起こす権限を持つのは州の司法長官のみであるため、ジョンはデータ侵害について企業を訴えることはできません。
- B. ジョンは、データ侵害の結果として被った金銭的損害を回復するために、データ侵害について企業を訴えることができ、また、状況によっては、金銭的損害を被ったかどうかに関係なく、法定損害賠償を求めることができます。
- C. CCPA ではデータ侵害に関する権利が規定されていないため、ジョンには企業を訴える権利がありません。
- D. ジョンはデータ侵害について企業を訴えることができますが、その対象となるのはデータ侵害の結果として実際に被った金銭的損害の回復のみです。

Answer: ([解答を表示する](#))

最新問題: 142

シナリオ

次の質問に回答するには、以下を使用してください。

あなたは、米国州 A の大都市にある主要病院 HealthCo の最高プライバシー責任者です。HealthCo は HIPAA の対象事業体であり、100,000 人以上の患者に医療サービスを提供しています。サードパーティのクラウドコンピューティング サービス プロバイダーである CloudHealth は、HealthCo に代わってこれらの個人の電子保護医療情報 (ePHI) を保存および管理しています。CloudHealth はデータを州 B に保存します。HealthCo と CloudHealth とのビジネス アソシエート契約 (BAA) の一環として、HealthCo はデータを適切に保護するために、業界標準の暗号化手法を含むセキュリティ対策を CloudHealth に実装することを要求しています。しかし、HealthCo は契約を締結する前に CloudHealth に対してデュー デリジェンスを実施しておらず、CloudHealth のセキュリティ対策の監査も実施していません。CloudHealth の従業員が最近フィッシング攻撃の被害者になりました。従業員が不審なメールのリンクをうっかりクリックしたため、HealthCo の患者 10,000 人以上の PHI が侵害され、その後、その情報がオンラインで公開されました。HealthCo のサイバーセキュリティチームは、犯人が他の病院に対して同様の攻撃を仕掛けた既知のハッカーであることをすぐに特定しました。この攻撃では、著名人や政治家などの公人の PHI が漏洩しました。

調査の過程で、HealthCo は、CloudHealth が契約条件に従って PHI を暗号化していなかったことを発見しました。さらに、CloudHealth は従業員にプライバシーやセキュリティに関するトレーニングを提供していませんでした。法執行機関は、HealthCo に対し、侵害に関する調査報告書と影響を受けた個人の PHI のコピーを提供するよう要求しました。

侵害の影響を受けた患者は、HealthCo 社が患者の ePHI を適切に保護しなかったため、漏洩したデータによって患者が多大な損害を被ったと主張して同社を訴えました。患者の弁護士は、侵害で漏洩した ePHI に関する証拠開示請求を提出しました。

弁護士の証拠開示要求に対する HealthCo の最善の対応は次のどれでしょうか？

- A. 原告に関する部分のみ編集した文書で回答する
- B. HIPAA プライバシー規則では支払い、治療、または医療業務の目的でのみ開示が許可されているため、要求を拒否します。
- C. 侵害された患者の記録をすべて原告の弁護士に引き渡す
- D. 限定的保護命令などの満足のいく保証の要求に応じる

Answer: D (メッセージを残す)

最新問題: 143

公正信用報告法 (FCRA) に基づき、信用履歴に基づいて雇用を拒否された人は何を受ける必要がありますか？

- A. 雇用主からの迅速な通知。
- B. 雇用主に再応募する機会。
- C. 複数の消費者信用情報機関 (CRA) からの情報。
- D. 消費者金融保護局 (CFPB) からの権利のリスト。

Answer: D (メッセージを残す)

<https://www.consumerfinance.gov/compliance/supervision-examinations/fair-credit-reporting-act-fcra-examination-procedures/> 2010年に議会はドッド＝フランク・ウォール街改革・消費者保護法 (ドッド＝フランク法) を可決し、FCRA (第15条(e)項 レッドフラッグガイドラインおよび規制) および第628条 (記録の廃棄) を除く) に基づく規則制定権限を消費者金融保護局 (CFPB) に付与しました。ドッド＝フランク法はまた、FCRAの2つの条項を改正し、不利な措置を講じたりリスクベースの価格設定に信用スコアが使用される場合に信用スコアおよび関連情報を開示することを義務付けました。

最新問題: 144

次の組織はすべて、医療保険の携行性と責任に関する法律 (HIPAA) の対象事業体として指定されていますが、次の組織は除きます。

- A. ヘルスケア情報センター
- B. 製薬会社
- C. 医療提供者
- D. 健康保険

Answer: (解答を表示する)

* 1974 年プライバシー法は、連邦政府機関による個人情報収集、使用、開示を規制する連邦法です。

* 1974 年のプライバシー法は、記録システムで維持される記録に適用されます。記録システムとは、個人の名前、または個人に割り当てられた識別番号、シンボル、その他の識別子によって情報を取得する機関の管理下にある記録のグループとして定義されます。

* 1974 年のプライバシー法は、個人に自分の記録にアクセスし、修正する権利を与え、機関に記録システムに関する通知を提供し、記録を保護するための安全策を確立し、記録の開示を特定の許可された目的に制限することを義務付けています。

* 1974 年のプライバシー法では、無許可の開示、通知の不掲載、アクセスや修正の許可の拒否など、法律違反に対する民事および刑事罰も規定されています。

* 1974 年プライバシー法では、個人情報を収集する前に機関が個人の同意を得ることを義務付けていません。ただし、1974 年プライバシー法では、収集の権限、収集の目的と使用、および情報を提供しない場合の影響について個人に通知することを機関に義務付けています。

参考文献: [1974年プライバシー法の概要]

最新問題: 145

シナリオ

次の質問に回答するには以下を使用してください

オットー氏は、プライバシー プログラムを担当する Filtration Station の取締役会に提出する報告書を準備中です。Filtration Station は、製薬会社に研究用フィルターやチューブ製品を販売する米国企業です。同社はワシントン州シアトルに本社を置き、米国およびアジア全土にオフィスを構えています。米国およびアジア太平洋地域の企業顧客に製品を販売しています。Filtration Station は、APEC プライバシー フレームワークの越境プライバシー ルール システムに参加しています。

残念ながら、Filtration Station は前四半期にデータ侵害に見舞われました。未知の第三者が Filtration Station のネットワークにアクセスし、米国に拠点を置くサードパーティのクラウド プロバイダーがホストする同社の人事データベース内の従業員に関するデータを盗むことができました。人事データは暗号化されています。Filtration Station は、サードパーティのクラウド プロバイダーを使用して、ビジネス マーケティング連絡先データベースもホストしています。マーケティング データベースはデータ侵害の影響を受けませんでした。データ侵害は、クラウド プロバイダーのシステム管理者がデータ自体に暗号化キーを保存したことが原因であるようです。

委員会は、データ侵害に関する情報と、プライバシー法および規制の新たな展開に関する最新情報が Filtration Station にどのように適用されるかに関する情報を Otto に提供するように求めました。委員会は、特にカリフォルニア州消費者プライバシー法 (CCPA) と侵害通知要件など、ニュースで取り上げられているさまざまな米国の州法および規制について最新情報を把握することに特に関心を持っています。

取締役会はオットー氏に、同社が新しいカリフォルニア州消費者プライバシー法 (CCPA) に準拠する必要があるかどうかを尋ねました。オットー氏は取締役会に何と答えるべきでしょうか？

- A. CCPA はカリフォルニア州に拠点を置く企業にのみ適用され、企業はコンプライアンスの義務を免除されます。
- B. そのビジネス連絡先情報は、CCPA によって管理される個人情報とみなされる可能性があります。
- C. 当社は CCPA の対象ですが、CPBR に準拠しているため、追加の手順を実行する必要はありません。
- D. カリフォルニア州司法長官が法律を施行すると決定した後にのみ、CCPA が会社に適用されます。

Answer: D (メッセージを残す)

最新問題: 146

古くなったデータプライバシー法における救済規定の目的は何ですか？

- A. 強制執行を受ける前に、企業が違反の疑いを修正するための限られた時間枠を与えること。
- B. 消費者が自分のデータが不適切に扱われたことを発見する時間を与える
- C. 州が一定期間内に正式な執行措置を開始できるようにする。
- D. 法律の特定の条項を定められた期間後に失効させること

Answer: A (メッセージを残す)

州のデータプライバシー法の是正規定により、企業は違反の疑いの通知を受け取った後、指定された期間内に法律違反を是正する機会が与えられます。この規定は、罰則や強制措置を直ちに課すのではなく、コンプライアンスを促進することを目的としています。

救済規定の主な側面:

* 通知および是正期間:

* 州当局による正式な執行措置が取られる前に、企業には、申し立てられた違反に対処するための期間 (例30 日間) が与えられます。

* コンプライアンスの促進:

* 是正規定は、軽微な違反や初回の違反に対して罰金や罰則を科されることなく、企業が是正措置を実施し、遵守を確保することを奨励します。

* 州別の例:

* カリフォルニア州消費者プライバシー法 (CCPA) には当初 30 日間の救済規定が含まれていましたが、後にカリフォルニア州プライバシー権法 (CPR) に基づいて制限されました。

* バージニア州の消費者データ保護法 (VCDPA) などの他の州法にも、救済規定が含まれています。

オプションの説明:

* A. 強制執行を受ける前に、企業に違反行為の是正のための限られた時間を与えること。これは正解です。是正規定は、強制措置を受ける前に企業が違反に対処する機会を与えることを目的として特別に設計されています。

- * B. 消費者が自分のデータが不適切に処理されたことを発見するための時間を与える:これは、データ侵害の通知に関連する消費者の権利を説明するものであり、救済規定を説明するものではありません。
- * C. 州が一定期間内に正式な執行措置を開始できるようにする: 是正規定は、執行措置を開始するのではなく、遅らせます。
- * D. 法律の特定の条項が定められた期間後に失効することを許可する:これは、救済条項ではなく、日没条項について説明しています。

CIPP/US 資料からの参照:

- * CCPA と CPRA: 是正規定とその施行における役割について説明します。
- * IAPP CIPP/US 認定テキスト: 州のプライバシー法における救済規定の目的と影響を強調します。

最新問題: 147

シナリオ

次の質問に回答するには、以下を使用してください。

ジェーンは米国市民で、カリフォルニアに本拠を置くジョーンズ研究所の上級ソフトウェアエンジニアです。ジョーンズ研究所は、米国防総省やその他の米国連邦政府機関への大手ソフトウェアサプライヤーです。ジェーンのマネージャーであるパトリックは、カリフォルニアに10年以上住んでいるフランス市民です。パトリックは最近、ジェーンが外国の諜報機関に秘密裏に企業秘密を送信しているインサイダーではないかと疑い始めました。パトリックは知らないうちに、FBIは匿名の内部告発者からすでにヒントを受け取っており、国家安全保障局と共同で、ジェーンが高度な外国スパイ活動に関与している可能性を調査しています。パンデミック以来、ジェーンは在宅勤務をしています。毎日のタスクを完了するために、彼女は会社のラップトップを使用しています。そのラップトップは、毎回の作業の後に、機器がジョーンズ研究所のものであり、制定されたプライバシーポリシーと雇用ハンドブックに従って監視される可能性があることを目立つように通知します。ジェーンには、ビジネス専用を使用している会社の携帯電話もあり、その条件は雇用契約で定義され、従業員ハンドブックで詳しく説明されています。プライバシーポリシーと従業員ハンドブックは、プライバシー法を専門とするカリフォルニアの評判の高い法律事務所によって毎年改訂されています。ジェーンは、私的な目的にのみ使用する個人用の iPhone も持っています。

Jones Labs のプライマリ データ センターはサンフランシスコにあり、Jones Labs のエンジニアによって内部的に管理されています。Amazon AWS によって管理されるセカンダリ データ センターは、災害復旧のために物理的には英国にあります。Jones Labs のモバイルデバイスのバックアップは、デンバーにある中規模のモバイル配信会社によって管理されており、コスト削減のため、物理的にはカナダにデータを保管しています。Jones Labs の MS Office ドキュメントは、Microsoft Office 365 データ センターに安全に保存されています。FISA のセクション 702 に基づき、NSA は外国情報監視裁判所の令状なしに次のどれを行うことができますか？

- A. AWS に、ジェーンと台湾在住の台湾国民との電子メール通信を公開するよう強制します。
- B. EU に居住する 2 人の中国人の間の電子メール通信を AWS に開示するよう強制する。
- C. ペルー在住のブラジル人とのパトリック氏の Skype 通話内容を Microsoft に開示するよう強制する。
- D. ジェーンに会社の携帯電話の PIN コードを開示するよう強制します。

Answer: (解答を表示する)

外国情報監視法 (FISA) 第 702 条に基づき、国家安全保障局 (NSA) は、外国情報収集の目的で米国外に居住する米国人以外の人物の通信を収集および分析する権限を有します。第 702 条では、一定の基準を満たしている場合、NSA は AWS や Microsoft などの米国ベースのサービス プロバイダーに、外国情報監視裁判所 (FISC) からの令状を必要とせずにデータへのアクセスを提供するよう強制できます。

セクション 702 の主な側面:

* 監視の範囲: セクション 702 は、米国外に居住する非米国人に適用されます。米国市民または米国内に居住する個人が非米国人と通信する場合でも、監視の対象とすることはできません。

* プロバイダーの義務: NSA は、データが外国諜報目的に関連している場合、米国を拠点とするサービス プロバイダー (AWS、Microsoft など) に、外国人が関与する通信に関する情報を開示するよう強制できます。

オプションの説明:

* A. AWS に、ジェーンと台湾在住の台湾国民との電子メールのやり取りを開示させる: 誤り。ジェーンは米国市民であり、通信の相手方が米国人以外の人であっても、セクション 702 を使用して米国人またはその通信を直接標的にすることはできません。

* B. EU 在住の中国人 2 名間の電子メール通信を AWS に開示させる: 正解。セクション 702 では、通信が AWS のような米国ベースのサービス プロバイダーによってホストされている場合でも、NSA が令状なしで米国外に居住する非米国人をターゲットにすることが許可されています。このシナリオはセクション 702 の適用範囲に直接該当します。

* C. ペルー在住のブラジル人とパトリックの Skype 通話内容をマイクロソフトに開示させる。

不正解です。パトリックはフランス国籍ですが、米国居住者です。セクション 702 は、米国に合法的に居住している個人をターゲットにするために使用することはできません。

* D. ジェーンに会社の携帯電話の PIN コードを開示するよう強制する: 誤り。セクション 702 は、個人ではなく、サービス プロバイダーが保持する電子通信データに適用されます。個人に PIN コードを開示するよう強制するには、裁判所が発行した召喚状や令状などの別の法的権限が必要になります。

法的枠組み:

* FISA の第 702 条: NSA に、米国を拠点とするサービス プロバイダーに、外国諜報目的で米国外に所在する非米国人のデータ収集に協力するよう強制する権限を与えます。

* ターゲットの制限: セクション 702 は、米国人または米国内に所在する人物に対して意図的にターゲットとして使用することはできません。

* サービスプロバイダー: 例としては、Amazon AWS、Microsoft、Google などの米国を拠点とする企業が含まれます。

Jones Labs の実践的な考慮事項:

Jones Labs は次のことを認識する必要があります。

* 米国を拠点とするプロバイダーに保存されているデータ (EU に所在する場合でも) は、依然としてセクション 702 の要求の対象となる可能性があります。

* 国際データ転送のコンプライアンスでは、米国の監視法の域外適用性を考慮して、GDPR などの EU プライバシー規制に準拠するための標準契約条項 (SCC) やその他の安全策を慎重に検討する必要がある場合があります。

CIPP/US 資料からの参照:

* FISA セクション 702 (50 USC § 1881a): 米国外に所在する米国人以外の人物をターゲットとする法的権限を概説しています。

* IAPP CIPP/US 認定テキスト: セクション 702 と、国際データを扱う米国ベースのサービスプロバイダーへの影響について説明します。

* シュレムス II 判決: 特に米国企業が海外に保管するデータに関して、米国の監視法と EU のプライバシー法の矛盾を強調しています。

最新問題: 148

どのような状況において、企業は暗黙の同意を前提として運営されているのでしょうか?

- A. 雇用主は応募者の履歴書に記載されている職業上の推薦者に連絡します
- B. オンライン小売業者は、新規顧客をデフォルトで電子メールリストに登録します。
- C. 家主は、記入済みの賃貸申込書の情報を使用して信用調査レポートを実行します。
- D. 小売店の店員がレジで顧客に郵便番号を尋ねる

Answer: (解答を表示する)

* 暗黙の同意とは、データ主体が明示的に表明した同意ではなく、データ主体の行動または不作為から推測される同意の形式です¹。

* 黙示の同意は、通常、契約の履行、データ管理者の正当な利益、またはデータ主体の合理的な期待のために処理が必要な場合など、特定の状況下では個人データを処理するための有効な根拠と見なされます²。

* ただし、適用される法律や規制によっては、健康、生体認証、遺伝データなどの機密性の高い個人データの処理やマーケティングコミュニケーションの送信には、黙示的な同意だけでは不十分な場合があります²。

* 米国には、データ処理に対する暗黙の同意の使用を規制する包括的な連邦プライバシー法はありませんが、異なる要件と制限を課す可能性のある業界固有の法律と州法が存在します³。

* 質問に示されているシナリオに基づくと、企業が黙示の同意を前提として活動する可能性が最も高い状況は、A です。雇用主が応募者の履歴書に記載されている職業上の推薦者に連絡します。

* これは、応募者が履歴書に自発的に推薦者の情報を提供することで推薦者との連絡に同意し、その連絡が応募者の資格と職務への適性を確認するという雇用主の正当な利益のために必要であると雇用主が合理的に推測できるためです4。

* その他の状況では、データ処理の種類と目的、および関連する法律や規制5に応じて、黙示の同意は必要なく、明示的な同意が必要になったり、データ主体にオプトアウトのオプションが提供されたりする場合があります。例:

* B. オンライン小売業者は、新規顧客をデフォルトで電子メール リストに登録します。これは、オンライン マーケティング担当者が商用電子メール メッセージを送信する前に受信者から積極的な同意を得ること、およびすべてのメッセージに明確で目立つオプトアウト メカニズムを提供することを義務付ける CAN-SPAM 法に違反する可能性があります5。

* C. 家主は、記入済みの賃貸申込書の情報を使用して信用調査を行います。これは公正信用報告法に違反する可能性があります。公正信用報告法では、家主は消費者レポートを取得する前に申込者から書面による許可を得て、それを提供する必要があります。

* 報告書のコピーと、報告書に基づいて不利な措置を講じた場合の権利の概要を通知します。

* D. 小売店の店員がレジカウンターで顧客に郵便番号を尋ねる。これはカリフォルニア州ソング ・ビバリー ・クレジットカード法に違反する可能性があります。この法律では、配送や詐欺防止などの特別な目的に必要な場合を除き、小売業者がクレジットカードで支払う顧客に個人識別情報を要求したり記録したりすることを禁止しています。

参照: 1: 黙示の同意 2: 同意 3: 米国民間部門プライバシー (CIPP/US) 4: [参照チェック: 求職者と雇用主のためのヒント] 5: [CAN-SPAM法: ビジネス向けコンプライアンス ガイド]: [消費者レポートの使用: 家主が知っておくべきこと]: [カリフォルニア州ソング ・ビバリー ・クレジットカード法]: [身元照会: 求職者と雇用主のためのヒント]: [CAN-SPAM法: ビジネス向けコンプライアンス ガイド]: [消費者レポートの活用: 家主が知っておくべきこと]: [カリフォルニア州ソング ・ビバリー ・クレジットカード法]

最新問題: 149

シナリオ

次の質問に回答するには、以下を使用してください。

Miraculous Healthcare は、カリフォルニア州とネバダ州に複数の拠点を持つ大規模な医療機関です。

Miraculous では通常、患者を直接治療しますが、この新しい取り組みのために、患者が電話アプリを介して現場の医師と仮想的に診察を受けられる遠隔医療予約の提供を開始することを最近決定しました。Miraculous は、医療行為のための高品質の遠隔医療アプリを作成し、そのアプリを医療行為のブランドで使用できるようにライセンス供与する会社である MedApps によって構築された製品を検討しています。MedApps は、クラウドでホストする

アプリの技術サポートを提供します。MedApps はまた、サービスを使用している他の医療行為と自分の行為を比較したい医療提供者向けに、オプションのベンチマーク サービスも提供しています。Riya は Miraculous のプライバシー責任者で、HIPAA およびその他の適用法に対する医療行為のコンプライアンスを担当しており、ベンダー契約を締結するために Miraculous の調達チームと協力しています。彼女は、ベンダーの審査やベンダー独自のコンプライアンス慣行の問い合わせ、ベンダー契約条件の交渉で調達を支援することもあります。Riya は現在、プライバシーの観点から MedApps アプリの適合性を検討しています。Riya は、Miraculous Healthcare のビジネス オペレーション チームから、MedApps のオプションのベンチマーク サービスを確認するよう依頼されています。特に懸念されるのは、Miraculous Healthcare が MedApps がホストするポータルに予約に関する情報をアップロードする必要があることです。MedApps がカリフォルニアを拠点とするアプリ ユーザーから CCPA に基づくアクセス要求を受け取った場合、その要求をどのように処理すればよいのでしょうか。

- A. MedApps は直ちにユーザーのデータの削除を開始する必要があります。
- B. MedAppsはプライバシー通知を読みやすい形式で提供する必要があります
- C. MedApps はカリフォルニアに拠点を置いていないため、リクエストを拒否する必要があります。
- D. MedApps は、処理の指示を得るためにリクエストを Miraculous に速やかに転送する必要があります。

Answer: ([解答を表示する](#))

カリフォルニア州消費者プライバシー法 (CCPA) に基づき、企業は消費者からのアクセス、削除、またはデータの処理方法に関する情報の要求に応じる必要があります。ただし、CCPA の下で企業が企業として行動しているか、サービス プロバイダーとして行動しているかによって、責任は異なります。

主な CCPA の定義:

* 仕事 :

* 個人情報の処理目的および手段を決定する主体。

* このシナリオでは、Miraculous Healthcare がビジネスとなります。なぜなら、Miraculous Healthcare は、ヘルスケア サービスの提供にアプリと関連データをどのように使用するかを決定するからです。

* サービスプロバイダー:

* 契約上の合意に従って企業に代わって個人情報を処理する事業体。

* MedApps は、Miraculous Healthcare に代わってアプリとデータをホストおよび管理しているため、サービス プロバイダーとして機能します。

サービス プロバイダーとして、MedApps は消費者データの取り扱い方法が制限されており、データ関連のリクエストについては企業 (Miraculous Healthcare) の指示に従う必要があります。したがって、MedApps がカリフォルニア在住のユーザーからアクセスまたは削除のリクエストを受け取った場合、そのリクエストを Miraculous Healthcare に転送する必要があります。Miraculous Healthcare は、CCPA に準拠した対応方法を決定する責任を負います。

オプションの説明:

* A. MedApps は直ちにユーザーのデータの削除を開始する必要があります。これは誤りです。CCPA の下では、MedApps はアクセスまたは削除の要求に独自に対応することはできません。サービス プロバイダーとして、Miraculous Healthcare の指示に従う必要があります。

* B. MedApps はプライバシー通知を読みやすい形式で提供する必要があります。これは質問とは無関係です。プライバシー通知を読みやすい形式で提供することは CCPA の要件ですが、アクセス要求の処理方法については規定されていません。

* C. MedApps はカリフォルニアに拠点を置いていないため、リクエストを拒否する必要があります。これは誤りです。CCPA は、事業体自体が物理的にカリフォルニアに所在しているかどうかに関係なく、カリフォルニア居住者の個人データを収集または処理する企業およびサービス プロバイダーに適用されます。

* D. MedApps は、処理に関する指示を得るために、リクエストを Miraculous に速やかに転送する必要があります。

これは正解です。CCPA では、サービス プロバイダーは企業と協力する必要があり、消費者のリクエストを企業に転送してガイダンスと対応を求めなければなりません。サービス プロバイダーとしての MedApps の役割は、Miraculous Healthcare の指示に従う義務を負っています。

CIPP/US 資料からの関連参考文献:

* CCPA セクション 1798.140(v): サービス プロバイダーを定義し、企業に代わって契約条件に従ってのみ個人情報を処理する義務を概説します。

* CCPA セクション 1798.105(c): 企業から指示がない限り、サービスプロバイダーは個人情報を削除する必要がないことを規定しています。

* IAPP CIPP/US 認定テキスト: CCPA に基づく企業とサービス プロバイダーの役割と、消費者の要求に対するそれぞれの責任について説明します。

実用的な考慮事項:

Riya は、Miraculous Healthcare のプライバシー責任者として、MedApps とのビジネス アソシエイト契約 (BAA) および CCPA 固有の契約条項で次の内容が明確に定義されていることを確認する必要があります。

* CCPA に基づいて消費者のリクエストを処理するプロセス。

* MedApps は、このようなリクエストがあった場合は Miraculous Healthcare に速やかに通知し、対応することが必要となります。

結論:

MedApps はサービス プロバイダーとして、CCPA のアクセスまたは削除要求に独自に対応する権限がありません。指示を得るために、Miraculous Healthcare に要求を転送する必要があります。

最新問題: 150

次のどれが APEC プライバシー フレームワークに含まれない原則ですか?

A. 個人情報の完全性。

- B. アクセスと修正。
- C. 危害を防ぐ。
- D. プライバシーを考慮した設計。

Answer: D (メッセージを残す)

説明/参考: [https://www.google.com/url?](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiqtJX4tPHvAhUQG-wKHUoGBgkQFjAHegQIBRAD&url=https%3A%2F%2Fwww.apec.org%2F-%2Fmedia%2FAPEC%2FPublications%2F2016%2F11%2F2016-CTI-Report-to-Ministers%2FTOC%2FAppendix-17-Updates-to-the-APEC-Privacy-Framework.pdf&usg=AOvVaw1Yysi4Ym_1VaCw1VZiB70a)

[sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiqtJX4tPHvAhUQG-wKHUoGBgkQFjAHegQIBRAD&url=https%3A%2F%2Fwww.apec.org%2F-%2Fmedia%2FAPEC%2FPublications%2F2016%2F11%2F2016-CTI-Report-to-Ministers%2FTOC%2FAppendix-17-Updates-to-the-APEC-Privacy-Framework.pdf&usg=AOvVaw1Yysi4Ym_1VaCw1VZiB70a](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiqtJX4tPHvAhUQG-wKHUoGBgkQFjAHegQIBRAD&url=https%3A%2F%2Fwww.apec.org%2F-%2Fmedia%2FAPEC%2FPublications%2F2016%2F11%2F2016-CTI-Report-to-Ministers%2FTOC%2FAppendix-17-Updates-to-the-APEC-Privacy-Framework.pdf&usg=AOvVaw1Yysi4Ym_1VaCw1VZiB70a)

最新問題: 151

FTC 法第 5 条によれば、自主規制には主に企業が行う権利が含まれますか?

- A. 裁定に関与する機関を決定する
- B. 強制措置が正当であるかどうかを判断する
- C. 業界の行動規範を遵守する
- D. 控訴決定に対する異議申し立て

Answer: (解答を表示する)

FTC 法第 5 条によれば、自主規制は主に企業が業界の行動規範を遵守する権利に関係しません。自主規制とは、業界または企業グループが消費者を保護し、公正な競争を促進するために、自主的に基準またはガイドラインを採用して施行するプロセスです。

FTC は、執行努力を補完し、市場で新たに発生する問題に対処する方法として、自主規制を奨励しています。また、FTC は自主規制プログラムを監視し、独自の行動規範を遵守しない企業や、そのようなプログラムへの参加を偽る企業に対して措置を講じることがあります。

参考資料:

- * 連邦取引委員会法第5条
- * 自主規制 | 連邦取引委員会
- * [IAPP CIPP/US 認定情報プライバシー専門家学習ガイド]、第 3 章、79 ページ

有効な **CIPP-US** 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集！ GoShiken.com が最新の **CIPP-US** 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (228**30%OFF**問題集溶と正解付きで **30%**w 特別割引コード:

Freepdfdumps)

最新問題: 152

シナリオ

次の質問に回答するには以下を使用してください

オットー氏は、プライバシー プログラムを担当するフィルトレーションステーションの取締役会に提出する報告書を準備している。フィルトレーションステーションは、製薬会社に研究用のフィルターやチューブ製品を販売する米国企業である。同社はワシントン州シアトルに本社を置き、米国全土にオフィスを構えている。

Filtration Station は、米国とアジア太平洋地域の企業顧客に製品を販売しています。Filtration Station は、APEC プライバシー フレームワークの越境プライバシー ルール システムに参加しています。

残念ながら、Filtration Station は前四半期にデータ侵害に見舞われました。未知の第三者が Filtration Station のネットワークにアクセスし、米国に拠点を置くサードパーティのクラウド プロバイダーがホストする同社の人事データベース内の従業員に関するデータを盗むことができました。人事データは暗号化されています。Filtration Station は、サードパーティのクラウド プロバイダーを使用して、ビジネス マーケティング連絡先データベースもホストしています。マーケティング データベースはデータ侵害の影響を受けませんでした。データ侵害は、クラウド プロバイダーのシステム管理者がデータ自体に暗号化キーを保存したことが原因であるようです。

委員会は、データ侵害に関する情報と、プライバシー法および規制の新たな展開に関する最新情報が Filtration Station にどのように適用されるかに関する情報を Otto に提供するように求めました。委員会は、特にカリフォルニア州消費者プライバシー法 (CCPA) と侵害通知要件など、ニュースで取り上げられているさまざまな米国の州法および規制について最新情報を把握することに特に関心を持っています。

取締役会はオットー氏に、同社が新しいカリフォルニア州消費者プライバシー法 (CCPA) に準拠する必要があるかどうかを尋ねました。オットー氏は取締役会に何と答えるべきでしょうか？

- A. カリフォルニア州司法長官が法律を施行すると決定した後にのみ、CCPA が会社に適用されます。
- B. 会社は CCPA の対象ですが、CPBR に準拠しているため、追加の手順を実行する必要はありません。
- C. そのビジネス連絡先情報は、CCPA によって管理される個人情報とみなされる可能性があります。
- D. CCPA はカリフォルニア州に拠点を置く企業にのみ適用されるため、企業はコンプライアンスを免除されます。

Answer: ([解答を表示する](#))

CCPA は、カリフォルニア州居住者の個人情報を収集するすべての企業に適用されます。企業の所在地は問いません¹。CCPA では、個人情報を、特定の消費者または世帯を直接的または間接的に識別、関連付け、説明、関連付けられることが合理的に可能、または関連付けられることが合理的に可能なあらゆる情報と広く定義しています²。特定の個人にリンクされている場合、これには名前、電子メール アドレス、電話番号、役職などのビジネス連絡先情報が

含まれる可能性があります3。したがって、オットーは取締役会に、ビジネス連絡先情報は CCPA の対象となる個人情報と見なされる可能性があり、通知の提供、消費者の権利要求の尊重、合理的なセキュリティ対策の実装など、CCPA の要件に準拠する必要がある場合があることを伝える必要があります4。参考文献:

* CIPP/US 練習問題 (サンプル問題)、質問 124、回答 C、説明 C。

* IAPP CIPP/US 認定情報プライバシー専門家学習ガイド、第 6 章、セクション 6.2、p. 181-182.

* カリフォルニア州消費者プライバシー法 (CCPA)、第 1798.140 条、サブセクション (o)。

* 企業向け CCPA コンプライアンス チェックリスト、セクション 2、サブセクション (a)。

最新問題: 153

米国盗聴法に基づく電話監視の一般的な禁止事項の例外はどれですか?

- A. コールセンター例外
- B. 企業間通信の例外
- C. 通常の業務上の例外
- D. インターネット通話例外

Answer: C (メッセージを残す)

米国盗聴法は、法定例外のいずれかが適用されない限り、有線、口頭、または電子通信の傍受および開示を禁止しています。これらの例外の 1 つは、通常の業務の過程の例外であり、これにより、雇用主またはサービス プロバイダーは、品質管理、トレーニング、セキュリティ目的など、通常の業務の過程で行われる通信を傍受できます。この例外は、個人的な電話やメールなど、業務に関係のない通信や、嫌がらせ、差別、報復などの他の理由で傍受される通信には適用されません。この例外の範囲と適用性は、状況、当事者の同意、および州法によって異なる場合があります。その他のオプションは、盗聴法の下では有効な例外ではありません。参照: 1、2、3、4

最新問題: 154

FTC は、プライバシー原則に違反していることが判明した企業と同意判決の交渉を頻繁に行います。これは関係する両当事者にどのような利益をもたらすのでしょうか?

- A. 罰金の額を標準化します。
- B. 監査要件が簡素化されます。
- C. 潜在的に有害な宣伝を回避します。
- D. 裁判にかかる費用を節約できます。

Answer: D (メッセージを残す)

プライバシー原則に違反していることが判明した企業と同意判決を交渉することは、裁判にかかる費用を節約することで、関係する双方に利益をもたらします。同意判決を選択することで、FTC と企業の両方が、裁判を含む時間と費用のかかる訴訟手続きを回避できます。このアプローチにより、問題をより効率的に解決でき、企業はより迅速に是正措置を講じることが可能です。さらに、公開裁判や長期にわたる法廷闘争から生じる可能性のある有害な評

判を回避するのも役立ちます。同意判決には罰則や罰金が含まれる場合もありますが、多くの場合、コンプライアンスを改善し、消費者のプライバシー権を保護するための対策を実施することに重点が置かれます。

最新問題: 155

訴訟に関係する文書（紙または電子）上の特定の個人情報を保護するために、裁判所は一般的にどのような慣行を要求していますか？

- A. ハッシュ
- B. 削除
- C. 編集
- D. 暗号化

Answer: C ([メッセージを残す](#))

最新問題: 156

1980年のプライバシー保護法はなぜ起草されたのですか？

- A. 新聞施設に対する警察の捜索に応じるため
- B. 新聞社に対する民事訴訟で検察官を支援する
- C. ホワイトカラー犯罪の起訴を支援する
- D. 警察による個人のプライバシー侵害から個人を保護するため

Answer: A ([メッセージを残す](#))

PPAは個人を保護しますが、PPAはZurcher判決に直接応えて起草されました。1978年、米国最高裁判所はZurcher対Stanford Daily事件で、法執行機関が捜査令状を取得してニュース編集室を捜索し、犯罪行為に関連する証拠を探ることができるとの判決を下しました。この判決により、このような捜索によってジャーナリストが政府の干渉を恐れずに職務を遂行し、情報を収集する能力が妨げられる可能性があるという懸念が生じました。

最新問題: 157

プライバシーに対する欧州のアプローチを支持する人の中に、プライバシー慣行の自主規制に懐疑的な人がいる主な理由は何ですか？

- A. 技術とセキュリティの向上に多額の資金を投入する必要があるかもしれない
- B. 業界はルールを作成と施行に十分厳格ではない可能性がある
- C. 新規事業主は規制を理解していない可能性がある
- D. プライバシーのために人権が無視される可能性がある

Answer: ([解答を表示する](#))

欧州のプライバシーに対するアプローチは、プライバシーを強力な法的保護と監視を必要とする基本的人権として認識することに基づいています。EUは、一般データ保護規則 (GDPR) や ePrivacy 指令など、個人データに関わるすべての分野と活動に適用される包括的かつ拘束力のあるプライバシー法を採用しています。また、EUには、プライバシー法の遵守を監視および強制する独立したデータ保護機関 (DPA) と、プライバシー問題に関するガイダンスと意

見を発行する欧州データ保護委員会 (EDPB) があります。EU は、第三国または国際機関に転送される個人データに対しても、適切なレベルのプライバシー保護を要求しています。対照的に、米国のプライバシーに対するアプローチは、連邦法と州法、業界の行動規範、消費者教育、市場の力の組み合わせに依存するセクター別および自主規制モデルに基づいています。

U. 米国には、個人データに関わるすべての分野と活動を網羅する、包括的かつ強制力のある単一の連邦プライバシー法がありません。その代わりに、米国には、健康、金融、児童、電子通信のプライバシーなど、特定の問題や分野に対処する連邦法と州法の寄せ集めがあります。米国では、個人データに関するすべての分野と活動を網羅する、包括的かつ強制力のある連邦プライバシー法が存在します。

S. また、連邦取引委員会 (FTC)、連邦通信委員会 (FCC)、保健福祉省 (HHS) など、プライバシー問題に関する管轄権を共有するさまざまな連邦および州の機関があります。米国はまた、プライバシーに関する自主的な行動規範、基準、ベスト プラクティスを開発して遵守する業界による自主規制に依存しています。米国では、データ主体が同意した場合、または転送がプライバシー シールドや標準契約条項などのメカニズムによってカバーされている限り、適切なレベルのプライバシー保護を要求せずに、個人データを第三国または国際組織に転送することも許可されています。

欧州のプライバシー保護アプローチを支持する人々の中には、プライバシー保護の自主規制に懐疑的な人々もいます。自主規制はデータ主体の権利と利益を保護するには効果的でも一貫性もなく、説明責任も十分ではないと考えているからです。自主規制では、業界がプライバシー規則を遵守したり、プライバシーを強化する技術や慣行を採用したりするのに十分なインセンティブや制裁が与えられない可能性があるかと主張しています。また、自主規制ではデータ主体の意見や期待が反映されない可能性があり、新しい技術やビジネス モデルによってもたらされる新たな複雑なプライバシー保護の課題に対処できないとも主張しています。また、自主規制の透明性と正当性、データ主体が権利を行使しプライバシー侵害の救済を求める能力についても疑問視されています。参考文献:

* IAPP CIPP/US 学習ガイド、第 1 章: 米国のプライバシー環境の概要、9-10、16-17 ページ

* IAPPウェブサイト、CIPP/US認証

* NICCSウェブサイト、米国認定情報プライバシー専門家 (CIPP/US) トレーニング

最新問題: 158

次の組織のうち、顧客に毎年プライバシー通知を提供する必要があるのはどれですか？

- A. ゴールデン ギャベル オークションハウス。
- B. フォーウィンズ部族大学。
- C. ブリージーシティ住宅委員会。
- D. キング郡貯蓄貸付組合。

Answer: ([解答を表示する](#))

最新問題: 159

連邦法では、13歳未満の未成年者の個人情報を収集するための次の要件のうちどれが定められていますか？

- A. 未成年者の親または保護者からの暗黙の同意、または未成年者からの積極的な同意。
- B. 未成年者の個人情報をオンラインで収集する前に、未成年者の親または保護者の同意を得ること。
- C. 未成年者にインターネットの使用を許可する場合など、未成年者の個人情報をオンラインで収集する前に、未成年者の親または保護者からの暗黙の同意を得ること。
- D. 未成年者の個人情報をオフライン（対面など）で収集する前に、親または保護者の同意を得ること。これは、オンラインでの同意の要件も満たします。

Answer: B (メッセージを残す)

児童オンラインプライバシー保護法 (COPPA) は、13歳未満の児童からの個人情報のオンライン収集と使用を規制する連邦法です。COPPAでは、児童向けのWebサイトやオンラインサービスの運営者、または児童から故意に個人情報を収集するWebサイトやオンラインサービスの運営者に対し、そのような情報を収集、使用、または開示する前に、検証可能な保護者の同意を得ることを義務付けています。検証可能な保護者の同意とは、児童から個人情報を収集する前に、児童の保護者が運営者の情報慣行について通知を受け、その慣行に同意することを保証する、あらゆる合理的な努力（利用可能なテクノロジーを考慮）を意味します。COPPAでは、保護者に児童の情報へのアクセスを提供すること、合理的なセキュリティ対策を維持すること、データ保持を制限することなど、運営者にその他の義務も課しています。参考文献: COPPA、IAPP CIPP/US 学習ガイド、第2章、セクション 2.3.1

最新問題: 160

次の組織のうち、顧客に毎年プライバシー通知を提供する必要があるのはどれですか？

- A. フォーウィンズ部族大学。
- B. ゴールデン ギャベル オークションハウス。
- C. キング郡貯蓄貸付組合。
- D. ブリッジーシティ住宅委員会。

Answer: C (メッセージを残す)

グラム・リーチ・ブライリー法 (GLBA) に基づく年次プライバシー通知要件は、例外の要件を満たさない限り、顧客から非公開の個人情報を収集し、それを非関連第三者に開示する金融機関に適用されます。金融機関とは、1956年銀行持株会社法第4条(k)で定義されているように、本質的に金融的な活動またはそのような活動に付随する活動に従事するあらゆる事業体です。キング郡貯蓄貸付金は、金銭の貸付と預金の受け入れに従事しているため、この定義に基づく金融機関です。したがって、例外の条件を満たさない限り、顧客に年次プライバシー通知を提供する必要があります。フォーウィンズトライバルカレッジ、ゴールデンギャベルオークションハウス、およびブリッジーシティ住宅委員会は、本質的に金融的な活動またはそのような活動に付随する活動に従事していないため、GLBAに基づく金融機関ではありません。したがって、GLBAに基づく年次プライバシー通知を顧客に提供する必要はありません。参考資料:

- * グラム・リーチ・ブライリー法第1条に基づく年次プライバシー通知要件の改正。背景、第2段落。
- * 17 CFR § 248.5 - 顧客への年次プライバシー通知の要求、パラグラフ (a) (1)。
- * IAPP CIPP/US 学習ガイド、65 ページ。

最新問題: 161

テレマーケティング販売規則に準拠する必要があるのはどの組織ですか？

- A. 非営利団体が自らの名義で呼びかける
- B. 営利組織および非営利組織が顧客を確立するために追加サービスを販売する場合
- C. 営利団体および営利テレファンドによる慈善活動の勧誘に関する
- D. 営利団体が企業と企業の間には拘束力のある契約がある場合に電話をかける

Answer: B (メッセージを残す)

最新問題: 162

次のどれが連邦優先の例ですか？

- A. ペイメントカード業界 (PCI) がペイメントカードデータに対してデータセキュリティ標準を自己規制および施行する能力。
- B. 米国連邦取引委員会 (FTC) が、さまざまな分野や業界にわたって不公正で欺瞞的な取引慣行を強制執行する能力。
- C. カリフォルニア州消費者プライバシー法 (CCPA) は、カリフォルニア州に物理的な実店舗を持たず、同州で事業を行っている企業を規制しています。
- D. 米国の CAN-SPAM (未承諾ポルノおよびマーケティングの攻撃の規制) 法は、電子メールマーケティングの送信者に厳しい義務を課す法律を各州が制定することを禁止しています。

Answer: (解答を表示する)

連邦法の優先権は、国家にとって重要な特定の問題 (州際通商など) において、連邦法が州法に優先するか、州法に取って代わることを許可する法理です。この法理は、連邦法が「国の最高法」であり、州の裁判官は連邦法に拘束されるという憲法の最高法規条項に基づいています。連邦法の優先権には、明示的と黙示的の2種類があります。明示的優先権は、連邦法が特定の種類の州法に優先することを意図していると議会が明示的に述べた場合に発生します。黙示的優先権は、州法が連邦法と矛盾する場合に発生します。これは、州法と連邦法の両方に同時に従うことが不可能な場合、または州法が連邦法の目的に干渉する場合、または連邦政府が規制分野を完全に占有している場合に発生します。

米国の「未承諾ポルノおよびマーケティングの攻撃の規制に関する法律 (CAN-SPAM)」は、明示的先取権の一例です。この法律は、商用電子メールメッセージを規制し、送信者に対する要件と違反に対する罰則を定めています。また、この法律は、虚偽または欺瞞を禁止する州法を除き、商用メッセージを送信するための電子メールの使用を明示的に規制する州法を明示的に先取権としています。つまり、州は、オプトイン同意の要求や追加のオプトアウトメカニズムの提供など、連邦法よりも厳しい義務を電子メールマーケティングの送信者に課す法律を制定することはできません。

したがって、CAN-SPAM 法がこの質問に対する正しい答えとなります。

その他のオプションは、連邦法による先取権の例ではありません。ペイメントカード業界 (PCI) がペイメントカードデータのセキュリティ基準を自主規制および施行する権限は、連邦法ではなく、民間セクターの取り組みです。米国連邦取引委員会 (FTC) がセクターや業界をまたいで不公正で欺瞞的な取引慣行を強制する権限は、州法による先取権ではなく、州の消費者保護法と共存できる同時権限です。カリフォルニア州に実店舗を持たず、同州で事業を行う企業を規制するカリフォルニア州消費者プライバシー法 (CCPA) は、連邦法によって先取権が定められていませんが、カリフォルニア州住民の個人情報を収集または販売する一定の基準を満たす事業体に適用される州法です。参考文献: 連邦法による先取権、連邦法による先取権とは?、連邦法による先取権の定義と意味、先取権、先取権の法的定義、CAN-SPAM 法、IAPP CIPP/US 学習ガイド、第 2 章。

最新問題: 163

特定の事件を審理するために裁判所はどのような管轄権を持つ必要がありますか?

- A. 主題管轄と規制管轄
- B. 主題管轄と専門管轄
- C. 対人管轄権と事物管轄権
- D. 人的管轄権と職業的管轄権

Answer: ([解答を表示する](#))

参照 :

~klett/chapter%25202%2520bl281%2520judicial%2520review%2520new.htm
+&cd=1&hl=en&ct=clnk&gl=pk&client=firefox-be

最新問題: 164

公民権法、妊娠差別禁止法、アメリカ障害者法、年齢差別禁止法、同一賃金法の共通点は何でしょうか?

- A. 雇用主は特定の従業員に対して合理的な配慮を提供することが義務付けられている
- B. 従業員が個人情報を利用する際に、雇用主は特定の階級に対して差別を行わないことが義務付けられている。
- C. 個人情報に関する問い合わせを制限することで、特定の従業員のプライバシー保護を実現しています。
- D. 雇用主が特定のクラスに属する従業員の個人情報を使用または開示することを許可する

Answer: B ([メッセージを残す](#))

最新問題: 165

FERPA によれば、学校はどのような場合に生徒の同意なしに記録を開示できるのでしょうか?

- A. 開示が第三者への電子メールを通じて行われえない場合
- B. 開示によって学生の学生番号が明らかにならない場合
- C. 学生の健康管理に携わる医療従事者への開示の場合

D. 開示が、学生が入学を希望する学校に成績証明書を提供することである場合

Answer: D (メッセージを残す)

FERPA によれば、開示が 34 CFR § 99.31 の例外のいずれかを満たす場合、学校は適格な学生の教育記録から個人を特定できる情報 (PII) を同意なしに開示することができます。

これらの例外の1つは、学生が入学を希望または意図している、またはすでに入学している他の学校への開示であり、開示が学生の入学または転校に関連する目的である場合です §4 CFR §

99.31(a)(2))。この例外により、学校は成績証明書、推薦状、または他の学校への入学または登録を容易にする可能性のあるその他の情報を開示できます。ただし、学校は、学生が開示を開始した場合を除き、開示について学生に通知するための合理的な努力を払う必要があります、要求に応じて開示された記録のコピーを学生に提供する必要があります §4 CFR §

99.34(a)(1))。参考文献 <https://studentprivacy.ed.gov/ferpa>

<https://studentprivacy.ed.gov/ferpa>

最新問題: 166

テレマーケティング販売規則では、組織が特定の消費者に対する Do-Not-Call 規則の例外を取得するには、どのような同意特性が整っていなければなりませんか？

A. 同意は書面で行われ、消費者に電話をかけることができる時間を明記し、署名されなければなりません。

B. 同意は書面で行われ、電話をかけられる番号と終了日が記載されていなければなりません。

C. 同意は書面で行われ、電話をかけることができる番号が記載され、署名されなければならない。

D. 同意は書面で行われ、終了日と通話可能な時間を明記する必要があります。

Answer: C (メッセージを残す)

[https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-](https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement)

[rule#writtenagreement](https://www.ftc.gov/business-guidance/resources/complying-telemarketing-sales-rule#writtenagreement) 書面による契約には何を含める必要がありますか？ 書面による契約には、次の内容のみを含める必要があります。 - 特定の販売者またはその代理人による録音済みメッセージを配信する電話を受信者が受信する意思があることを示す明確な証拠、そのようなメッセージを配信できる電話番号、および - 通話受信者の署名。

有効な **CIPP-US** 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集！ GoShiken.com が最新の **CIPP-US** 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (228**30%OFF**問題集溶と正解付きで **30%**w 特別割引コード:

Freepdfdumps)

最新問題: 167

政府機関と相手方当事者間の合意を正式なものとする、裁判官によって承認された法的文書は何と呼ばれますか？

- A. 同意判決
- B. 毅然とした態度で臨むことを決意する
- C. 審判のライダー
- D. コモンロー上の判決

Answer: A (メッセージを残す)

同意判決とは、政府機関と相手方当事者の間の紛争を、双方が罪や責任を認めることなく解決する法的文書です。裁判官によって承認され、裁判所命令と同じ効力を持ちます。同意判決には、コンプライアンス、監視、報告、是正などの条件が含まれる場合があります。同意判決は、連邦取引委員会 (FTC)、環境保護庁 (EPA)、司法省 (DOJ) などの連邦機関が提起した民事執行訴訟の解決によく使用されます。参考文献:

- * IAPP用語集、同意判決」の項目
- * [IAPP CIPP/US 学習ガイド]、39 ページ、セクション 2.1.3
- * [IAPP CIPP/US Body of Knowledge]、9ページ、セクションB.1.a

最新問題: 168

Acme Student Loan Company は、個人が請求書を支払う可能性があるか、または支払いを怠る可能性があるかを判断する人工知能アルゴリズムを開発しました。アルゴリズムによって支払いを怠る可能性が高いと判断された人には、支払いを催促する電話が頻繁に送信されますが、支払いを怠る可能性が低い人には、支払い催促の電話は送信されません。

Acme Student Loan Company がこのように人工知能を使用することに対するプライバシーの懸念を最も正確に反映しているのは、次のどれですか？

- A. アルゴリズムが自動決定エンジンに影響を与えるリスク要因を使用する場合、Acme は、アルゴリズムが出力内の保護されたクラスに異なる影響を与えないようにする必要があります。
- B. アルゴリズムがリスク要因と公開情報に基づいて自動的に決定を行う場合、Acme はアルゴリズムが保護されたクラスに異なる影響を及ぼすかどうかを判断する必要はありません。
- C. アルゴリズムの方法論が消費者に公開されている場合、Acme が保護されたクラスに異なる影響を与えることは許容されます。
- D. アルゴリズムが保護されたクラスに関する情報を使用して自動決定を行う場合、Acme はアルゴリズムが出力内の保護されたクラスに異なる影響を及ぼさないことを保証する必要があります。

Answer: D (メッセージを残す)

正解は D です。アルゴリズムが保護クラスに関する情報を使用して自動決定を行う場合、Acme は出力においてアルゴリズムが保護クラスに不均衡な影響を及ぼさないことを保証する必要があります。公正信用報告法 (FCRA) は、消費者を、信用レポートを使用する債権者やその他の企業による不公平、不正確、差別的な扱いから保護します。FCRA は、債権者が

保護クラスに関する情報(人種、肌の色、宗教、国籍、性別、婚姻状況、年齢、または公的扶助プログラムから収入を得ているかどうかなど)を使用して信用に関する決定を行うことを禁止しています。Acme Student Loan Company の場合、アルゴリズムは保護クラスに関する情報を使用して、支払いリマインダーの電話をかけるかどうかの自動決定を行っています。これは、有色人種や低所得者などの保護クラスに不均衡な影響を及ぼす可能性があります。たとえば、有色人種は、他の人種の人と同じようにローンを返済する可能性がある場合でも、債務不履行のリスクがあると特定される可能性が高くなります。Acme Student Loan Company は、アルゴリズムが保護されたクラスに不均衡な影響を与えないようにする必要があります。これは、次のようなさまざまな方法で実行できます。

- * 導入前と導入後にアルゴリズムの精度、公平性、偏りをテストする
- * 消費者にデータの使用に関する通知と同意のオプションを提供する
- * 消費者が自分のデータにアクセスし、修正、削除できるようにする
- * アルゴリズムの説明責任と監視メカニズムの実装
- * 適用される法律および規制の遵守の確保

参考文献: <https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms>
<https://pupuweb.com/iapp-cipp-us-qa-privacy-concerns-acme-student-loan-company-artificial-intelligence/>

最新問題: 169

シナリオ

次の質問に回答するには、以下を使用してください。

ある晩、マットは息子の寝室に行って、息子がベッドに寝そべってノートパソコンを打っているのを見つけた。ネットワークの調子はいいかい？」とマットは期待を込めて尋ねた。

「いいえ」少年は言った。アンケートに答えているところです。」

マットは息子の肩越しに自分のコンピューターの画面を見た。どんな調査？」私の意見についての質問だよ。」

「ちょっと見てみよう」とマットは言い、息子がすでに答えた質問のリストを読み始めた。政府と市民権についての意見を聞いているんだ。ちょっと変だな。君はまだ10歳なのに。」マットは、どうしてこのアンケートのウェブラックが息子のメールの受信箱に入ってしまったのか不思議に思った。このメッセージは息子に間違えて送られたのかもしれないと思い、開いて読んでみた。このメッセージは、リーダーシッププロジェクトという団体から送られてきたもので、内容と画像から子供向けであることがわかった。マットが読み進めると、アンケートに答えた子供は自動的に、有名なリーダーに関するシリーズの最初の本が当たるコンテストに登録されることがわかった。

マットにとって、これは明らかに子供たちに商品やサービスを売り込むためのマーケティング戦略に思えました。彼は息子に、アンケートに答えるために自分自身の情報を提供するよう求められたかどうか尋ねました。息子は、名前、住所、電話番号、生年月日を尋ねられ、好きなゲームやおもちゃについての質問に答えるよう求められたと答えました。

マットは心配していました。マーケティング担当者が息子からこのような方法で情報を収集することが合法かどうか疑問に思いました。その後、息子の受信箱に子供向けの商品を宣伝するマーケティング担当者からの他のいくつかの商業メールが届いていることに気づき、この事件を適切な当局に報告する時だと判断しました。

マーケティング担当者は、COPPA の「[セーフハーバー](#)」要件を満たすために、プライバシー管理プログラムをどのように変更するのが最善でしょうか。

- A. 承認された自主規制プログラムに参加することにより
- B. 消費者のプライバシーに対するセキュリティリスクを定期的に評価することにより
- C. メールの内容についてFTCの承認を得ることにより
- D. COPPAプライバシー通知をウェブサイトで公開することにより

Answer: C ([メッセージを残す](#))

最新問題: 170

シナリオ -

次の質問に答えるには、以下を使用してください。

ジェーンは米国市民で、カリフォルニアに拠点を置くジョーンズ ラボの上級ソフトウェアエンジニアです。ジョーンズ ラボは米国国防総省やその他の米国連邦政府機関にソフトウェアを供給する大手企業です。ジェーンのマネージャーであるパトリックはフランス市民で、カリフォルニアに 10 年以上住んでいます。パトリックは最近、ジェーンが外国の諜報機関に秘密裏に企業秘密を漏らしている内部関係者ではないかと疑い始めました。パトリックは知りませんでした。FBI はすでに匿名の内部告発者からヒントを得ており、国家安全保障局と共同でジェーンが高度な外国スパイ活動に関与している可能性を調査しています。

パンデミック以来、ジェーンは在宅勤務をしています。彼女は日々の業務をこなすために会社のノートパソコンを使用していますが、ログインするたびに、機器はジョーンズ ラボの所有物であり、制定されたプライバシー ポリシーと雇用ハンドブックに従って監視される可能性があることが目立つように表示されます。ジェーンは会社の携帯電話も所有しており、これは仕事にのみ使用しています。その条件は雇用契約で定義され、従業員ハンドブックで詳しく説明されています。プライバシー ポリシーと従業員ハンドブックは、プライバシー法を専門とするカリフォルニアの評判の高い法律事務所によって毎年改訂されています。ジェーンは私用 iPhone も所有しており、私的な目的にのみ使用しています。

ジョーンズ ラボのプライマリ データ センターはサンフランシスコにあり、ジョーンズ ラボのエンジニアが社内で管理しています。セカンダリ データ センターは Amazon AWS によって管理されており、災害復旧のために物理的には英国にあります。ジョーンズ ラボのモバイル デバイスのバックアップは、デンバーにある中規模のモバイル ディフェンス会社によって管理されており、コスト削減のため物理的にはカナダにデータを保管しています。ジョーンズ ラボの MS Office ドキュメントは、アイルランドにある Microsoft Office 365 データ センターに安全に保管されています。ジョーンズ ラボの製造データは台湾に保管されており、米国には拠点のない現地のサプライヤーによって管理されています。

ジェーンの会社の携帯電話から GPS 位置情報データを調べる前に、パトリックはまず何をすべきでしょうか？

- A. 電話消費者保護法に従ってジェーンから事前の同意を得る
- B. 信頼できる擁護団体と協力して、職場のプライバシーに関する新たなベストプラクティスを改訂します。
- C. 法執行機関からの召喚状、または裁判所命令を取得し、Jones Labs に GPS 地理位置データの収集を指示します。
- D. そのような活動がジェーンの雇用契約または会社の従業員プライバシー ポリシーで許可されていることを確認します。

Answer: D (メッセージを残す)

カリフォルニア州では、勤務時間中に従業員を追跡することは合法です。ただし、カリフォルニア州民は憲法でプライバシーの権利を有しています。したがって、従業員を追跡する予定がある場合は、労働組合の協定に違反していないこと、および追跡ポリシーが文書化されていることを確認してください。」 <https://www.workyard.com/employee-time-tracking/gps-tracking-employees-laws>

最新問題: 171

米国の連邦差別禁止法が民間部門の従業員のプライバシーをどのように保護しているかを最もよく説明しているのは次のどれですか？

- A. 採用候補者の面接時間を制限します。
- B. 雇用主が従業員について収集できる情報の種類を制限します。
- C. 多様なスキルと興味を持つ従業員の労働力を促進します。
- D. 安全で快適な作業環境を規定します。

Answer: B (メッセージを残す)

最新問題: 172

次の法律のうち、従業員の身元調査の規制に関係しないものはどれですか？

- A. 公民権法。
- B. グラム・リーチ・ブライリー法 (GLBA)。
- C. 米国公正信用報告法 (FCRA)。
- D. カリフォルニア州調査消費者報告機関法 (ICRAA)。

Answer: B (メッセージを残す)

従業員の身元調査の規制に関係しない法律は、B. グラム・リーチ・ブライリー法 (GLBA) です。GLBA は、銀行、保険会社、証券会社などの金融機関が収集、使用、または共有する金融情報のプライバシーとセキュリティを規制する連邦法です。

GLBA は、雇用目的で消費者報告機関から財務情報を取得する金融機関でない限り、従業員の身元調査には適用されません。その場合、雇用主は GLBA の通知およびオプトアウト要件、ならびに消費者レポートの使用に関する FCRA の要件に従う必要があります。参考資料:

* [IAPP CIPP/US 学習ガイド]、第 4 章: 職場のプライバシー、pp. 113-114。

* IAPP CIPP/US Body of Knowledge、セクション IV: 職場のプライバシー、サブセクション A: 従業員のプライバシーの期待、トピック 3: 経歴調査。
* IAPP CIPP/US 練習問題、質問 150。

最新問題: 173

「電子情報開示」の規則は主に次のどれを防止しますか？

- A. ビジネス慣行と技術的安全対策の矛盾
- B. 不適切なデータ保持方法による情報の損失
- C. 従業員が個人所有のデバイスを仕事に利用する慣行
- D. 組織のデータ保持プログラムの違反

Answer: B (メッセージを残す)

最新問題: 174

1986 年の電子通信プライバシー法で禁止されている行為はどれですか？

- A. メッセージの送信者または受信者の同意を得て保存された通信にアクセスする
- B. 従業員の個人的な電話通話を監視する
- C. 電子通信の傍受および保存された通信への不正アクセス
- D. 従業員の電話通話をすべて監視

Answer: C (メッセージを残す)

最新問題: 175

Global Manufacturing Co の人事部は最近、新しいソフトウェア ツールを購入しました。このツールは、メールをスキャンして候補者の発言や候補者について言われている内容を確認し、幹部候補を評価するのに役立ちます。これにより、人事部は自動化された「B60 度評価」を行えるようになり、候補者の考え方や行動、同僚や直属の部下が候補者について何を言っているか、候補者同士のやり取りがどの程度うまくいっているかを知ることができます。この新しいソフトウェアを導入する際に人事部門が行う最も重要なステップは何ですか？

- A. ソフトウェアが保護されたグループに対して意図せず差別を行わないようにします。
- B. 従業員が組織のシステムでこのソフトウェアを実行して電子メール システムをスキャンしている限り、従業員にはプライバシーの権利がないことを説明するプライバシー通知がソフトウェアに含まれていることを確認します。
- C. 従業員が従業員ハンドブックを読んで署名したことを確認します。従業員ハンドブックには、EEOC によって施行される保護対象グループや法律に関係なく、組織のシステムを使用している限り、プライバシーの権利がないことが記載されています。
- D. 従業員に、電子メールがソフトウェアによってスキャンされ、自動プロフィールが作成されることを通知します。

Answer: A (メッセージを残す)

説明/参照: <https://www.beckage.com/tag/artificial-intelligence/>

最新問題: 176

1980年のプライバシー保護法はなぜ起草されたのですか？

- A. 新聞社に対する民事訴訟で検察官を支援する
- B. 新聞施設に対する警察の捜索に応じるため
- C. ホワイトカラー犯罪の起訴を支援する
- D. 警察による個人のプライバシー侵害から個人を保護するため

Answer: D ([メッセージを残す](#))

最新問題: 177

次のすべての慣習法上の不法行為は、米国法の下では従業員のプライバシーに関連しますが、次の例外はありません。

- A. 精神的苦痛を与えること。
- B. 隔離への侵入。
- C. 名誉毀損
- D. 変換。

Answer: B ([メッセージを残す](#))

説明/参照: https://en.wikipedia.org/wiki/Privacy_law

最新問題: 178

2011年、FTCは、ソーシャルネットワーキングサービス Google Buzz に関して Google との和解を発表しました。FTCは、サービスを開始する過程で、同社が次のすべてを行ったと主張しましたが、次の行為は除きます。

- A. 独自のプライバシーポリシーに違反しました。
- B. 不正な商行為に従事した。
- C. セーフハーバー原則に準拠できませんでした。
- D. 十分なセキュリティ保護手段を採用できませんでした。

Answer: ([解答を表示する](#))

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

最新問題: 179

シナリオ

次の質問に回答するには、以下を使用してください。

米国を拠点とする新興企業が新しいゲームアプリケーションを販売しています。ある日、同社のCEOは、EUを拠点とする著名な小売パートナーから緊急の手紙を受け取りました。手紙には、EU居住者が申し立てた未解決の苦情がきっかけとなり、小売業者のデータ処理慣行に関する監督当局による調査が進行中であることが記されていました。

申立人は、小売業者が彼女の個人データを米国の当事者に同意なく不適切に開示したと非難しています。さらに申立人は、EUを拠点とする小売業者が、彼女の同意の撤回と個人データの消去要求に応じなかったと非難しています。米国を拠点とするスタートアップ企業である貴社は、EUを拠点とする小売パートナーからこの消去要求について通知されていませんで

した。苦情を調査している監督当局は、関係者が調査に協力しない場合はデータフローを停止すると脅迫しています。手紙は、「当社から受け取ったすべての個人データを特定して、直ちに行動してください」という緊急の要請で締めくくられています。これは重要なパートナーシップです。会社の幹部は、その最大のファンが西ヨーロッパから来ていることを知っています。そして、この小売業者は、スタートアップの急速な市場浸透の主な原因です。会社のデータプライバシーリーダーとして、あなたは小売業者との関係の重要性に敏感です。

一般データ保護規則 (GDPR) では、米国を拠点とするスタートアップ企業はどのように分類される可能性が高いでしょうか？

- A. データ管理者として
- B. データ管理者として
- C. データスーパーバイザーとして
- D. データ処理者として

Answer: C (メッセージを残す)

最新問題: 180

公正かつ正確な信用取引法 (FACTA) に基づき、顧客の信用報告書の紙のフォルダーを保有する自動車ディーラーにとって最も適切な措置は何ですか？

- A. レッドフラッグルールに従い、顧客にレポートを郵送する
- B. 廃棄規則に従い、報告書を裁断する
- C. 報告書を安全な電子ファイルに転送することでセーフガードルールに従う
- D. レポートが保存されていることを顧客に通知することでプライバシールールに従う

Answer: D (メッセージを残す)

最新問題: 181

FERPA によれば、学校はどのような場合に生徒の同意なしに記録を開示できるのでしょうか？

- A. 開示が第三者への電子メールを通じて行われえない場合
- B. 開示によって学生の学生番号が明らかにならない場合
- C. 学生の健康管理に携わる医療従事者への開示の場合
- D. 開示が、学生が入学を希望する学校に成績証明書を提供することである場合

Answer: D (メッセージを残す)

FERPA によれば、開示が 34 CFR § 99.31 の例外のいずれかを満たす場合、学校は適格な学生の教育記録から個人を特定できる情報 (PII) を同意なしに開示することができます。

これらの例外の1つは、学生が入学を希望または意図している、またはすでに入学している他の学校への開示であり、開示が学生の入学または転校に関連する目的である場合です §4 CFR §

99.31(a)(2))。この例外により、学校は成績証明書、推薦状、または他の学校への入学または登録を容易にする可能性のあるその他の情報を開示できます。ただし、学生が開示を開始した場合を除き、学校は開示について学生に通知するための合理的な努力を払う必要があります、要

求に応じて開示された記録のコピーを学生に提供する必要があります (34 CFR § 99.34(a)(1))。参照: <https://studentprivacy.ed.gov/ferpa>
<https://studentprivacy.ed.gov/ferpa>

有効な **CIPP-US** 問題集は GoShiken.com が提供された合格しやすい CIPP-US 試験問題集！ GoShiken.com が最新の **CIPP-US** 試験問題集を提供しています。GoShiken.com CIPP-US 試験問題は最新で、解答が正確でございます。最新の GoShiken.com CIPP-US 問題集をゲットする人はこちら: <https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (**22830%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 182

シナリオ -

次の質問に答えるには、以下を使用してください。

ミラキュラス ヘルスケアは、カリフォルニア州とネバダ州に複数の拠点を持つ大規模な医療機関です。ミラキュラスでは通常、患者を直接診察しますが、最近、電話アプリを介して患者が現場の医師と仮想的に診察を受けられる遠隔医療の診察を開始することを決定しました。この新しい取り組みのために、ミラキュラスは、医療現場向けの高品質な遠隔医療アプリを開発し、そのアプリを医療現場のブランドで使用できるようにライセンス供与する企業、MedApps が開発した製品を検討しています。MedApps は、クラウドでホストするアプリの技術サポートを提供しています。また、MedApps は、サービスを使用している他の医療現場と自社の医療現場を比較したい医療提供者向けに、オプションのベンチマーク サービスも提供しています。

Riya は Miraculous のプライバシー責任者で、HIPAA やその他の適用法への準拠を担当しており、Miraculous の調達チームと協力してベンダー契約を締結しています。調達チームを支援してベンダーの審査やベンダーのコンプライアンス慣行の調査を行ったり、ベンダー契約の条件を交渉したりしています。Riya は現在、プライバシーの観点から MedApps アプリの適合性を検討しています。

Riya は、Miraculous Healthcare のビジネス オペレーション チームから、MedApps のオプションのベンチマーク サービスを確認するよう依頼されました。特に懸念されるのは、Miraculous Healthcare が MedApps がホストするポータルに予約に関する情報をアップロードする必要があることです。

Miraculous が遠隔医療アプリを使用する前に考慮しなければならない HIPAA コンプライアンスの問題は何ですか？

- A. HIPAA では、対面予約データを第三者と共有する前に Miraculous が患者の同意を得ることが義務付けられています。
- B. HIPAA では、対面予約データをクラウドでホストすることは許可されていません。

C. HIPAA では、医療提供者がクラウド ホスティング サービスを使用することは許可されていません。

D. HIPAA では、Miraculous と MedApps がビジネスアソシエイト契約を締結することが義務付けられています。

Answer: D (メッセージを残す)

Valid CIPP-US Dumps shared by GoShiken.com for Helping Passing CIPP-US Exam!
GoShiken.com now offer the **newest CIPP-US exam dumps**, the GoShiken.com CIPP-US exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com CIPP-US dumps with Test Engine here:

<https://www.goshiken.com/IAPP/CIPP-US-mondaishu.html> (**228** Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)