模擬試験

2018 年 5 月版

目次

はじめに

これは EXIN Privacy & Data Protection Foundation (PDPF.JP)試験の模擬試験です。この試験は EXIN 試験の規則および規定を適用します。

この試験では 40 問が多肢選択形式で出題されます。各問題には、選択肢が複数ありますが、そのうち正解は 1 つのみです。

この試験の最高点は 40 点です。正解 1 つにつき 1 点とします。26 点以上獲得すると合格となります。

試験時間は 60 分です。

ご健闘を祈ります。

模擬試験

1 / 40
個人データの違法な収集、保存、改変、開示、拡散は、犯罪であると欧州の法律で規定されています。

この犯罪の種類はどれですか？

A) コンテンツ関連犯罪
B) 金融犯罪
C) 知的財産犯罪
D) プライバシー犯罪

2 / 40
プライバシーとデータ保護はどのように関連していますか？

A) データ保護はプライバシーの一部である
B) プライバシーはデータ保護の一部である
C) プライバシーとデータ保護は同じである
D) データ保護がなければプライバシーは保てない

3 / 40
GDPRの**主な**目的は何ですか？

A) EU加盟国が自国の法律を制定するための基盤となること
B) EU域内の個人のプライバシーの権利を非EU加盟国に尊重させること
C) プライバシーを誰もが持つ基本的人権として確保すること
D) EU域内の個人のデータ保護を強化して統一すること

4 / 40
GDPRは個人データの保護に関連します。

個人データの定義は何ですか？

A) 識別された、または識別可能な自然人に関連するあらゆる情報
B) EU市民が保護したいと思うあらゆる情報
C) 人種や民族背景、宗教的見解、健康や性的習慣に関するデータを直接的または間接的に明らかにするデータ
D) 情報の機密性、完全性、可用性の維持

5 / 40
GDPRによると、機微データに分類される個人データはどれですか？

A) クレジットカードの詳細
B) 労働組合員資格
C) パスポート番号
D) 社会保障番号

6 / 40
GDPRに規定された個人データの「取扱（処理）」の定義は何ですか？

A) 個人データに対して実施できるすべての操作
B) 個人データに対して実施できる、消去と破棄以外のすべての操作
C) データをソーシャルメディアで共有する操作、もしくは、データをメール添付またはインターネット経由で送付する操作のみ
D) 個人データを収集した目的のために使用する操作のみ

7 / 40
「*第51条の規定に基づいて加盟国により設立された独立した公共機関*」

これはデータ保護におけるどの役割の定義ですか？

A) 管理者（コントローラ）
B) 取扱者
C) 監督機関
D) 第三者

8 / 40
GDPRでは、告知に基づく同意（インフォームドコンセント）は個人データを取扱うための適法的根拠です。同意を得た取扱い目的は文書化する必要があります。

データ主体の同意を得なければならないのは、個人データを取扱う場合のどの段階ですか？

A) 取扱い目的の詳細が示された後で、かつ個人データを収集する前
B) 取扱い目的の詳細が作成されて表示される前
C) 個人データを取扱う前
D) 個人データが公表されるかまたは拡散される前

9 / 40
GDPRは比例性と補完性の原理を基礎としています。

この文脈での「比例性」の意味は何ですか？

A) 個人データは目的の仕様に従ってのみ取扱いが可能である
B) 個人データは、明示的かつ告知に基づく同意がなければ再利用してはならない
C) 個人データは、他に目的を達成する手段がない場合にのみ取扱うことが可能である
D) 個人データは、目的に照らして適切であり、関連性があり、過度であってはならない

10 / 40
個人データの取扱いは一定の品質要件を満たさなければなりません。

GDPRが定義する品質要件に含まれるのはどれですか？

A) 取扱ったデータはアーカイブに入れなければならない
B) 取扱ったデータは暗号化しなければならない
C) 取扱ったデータは索引付けしなければならない
D) 取扱ったデータは関連付けしていなければならない

11 / 40
個人データを取り扱う場合は常に比例性と補完性を確認する必要があります。

取り扱い中の個人データの要件はどれですか？

A) 定義された目標の達成に必要なものに常に限定する必要があり、また、「干渉性」が最低限のデータに制限する必要がある
B) 可能な限り少人数の従業員が取扱わなければならず、また、取り扱う従業員は管理者（コントローラ）または提携会社の下で作業しなければならない
C) あらかじめ決められたストレージサイズに限定する必要があり、使用するシステムは管理者（コントローラ）が資金調達をする必要がある
D) 可能な限り少数の目的に使用しなければならず、また、取扱者の敷地外では使用してはならない

12 / 40
「管理者（コントローラ）は、（略）各具体的取扱いの目的に必要な個人データのみが取り扱われることを保証するための適切な技術的及び組織的対策を実施しなければならない。」

これはGDPRのどの用語の定義ですか？

A) コンプライアンス
B) データ保護バイデフォルト
C) データ保護バイデザイン
D) 組込保護

13 / 40
GDPRでは、個人データの不正な開示や個人データへの不正アクセスはどのように呼ばれますか？

A) 機密性侵害
B) データ侵害
C) インシデント
D) セキュリティ　インシデント

14 / 40
機微な個人データのデータ侵害が発生したことが確認されました。

GDPRによると、このデータ侵害は最終的に誰に報告をする必要がありますか？

A) 監督機関
B) データ保護責任者(DPO)
C) その部門のマネージャ
D) 警察

15 / 40
バックアップの実行中にデータサーバのディスクがクラッシュしました。データとバックアップの両方が失われました。ディスクには個人データが含まれていましたが、機微データはありませんでした。

このインシデントの種類は何ですか？

A) データ侵害
B) セキュリティ侵害
C) セキュリティ　インシデント

16 / 40
労働組合のある従業員が、組合員宅に送付するニュースレターのドラフトを完成させるために自宅に持ち帰りました。ドラフトと送付先リストを入れたUSBスティックを紛失しました。

このデータ侵害は、特に誰に報告すべきですか？

A) 送付先リストに記載された組合員全員
B) 労働組合のスタッフ
C) 警察

17 / 40
あるソーシャルサービス組織は、クライアントを管理するための新しいデータベースを設計し、必要な配慮（診療）を計画しています。

監督機関に許可を申請するためにとるべき最初の重要なステップに含まれるのはどれですか？

A) クライアントに関するデータ、また、必要かつ提供される配慮（ケア）の量と種類に関するデータを収集する
B) データ保護影響評価(DPIA)を実施して、意図する取扱いのリスクを評価する
C) 個人データの意図する取扱いについて、クライアントの同意を得る

18 / 40
データ主体が常にデータ侵害の通知を受ける必要があるのはどのような場合ですか？

A) EU域内に所在しない取扱者の施設で個人データが取扱われた場合
B) 個人データは、管理者（コントローラ）が送信した取扱契約書の草案に同意した当事者によって取扱われたが、まだ署名していない場合
C) 個人データが取扱われたシステムが攻撃され、ストレージ装置が損傷した場合
D) 侵害がデータ主体のプライバシーに有害な結果をもたらす重大な可能性がある場合

19 / 40
あるオランダの管理者（コントローラ）は、監督機関に相談せずに、北アフリカの国の取扱者に機微な個人データの取扱いを委託していました。これが発覚し、管理者は監督機関から処罰を受けました。6か月後、監督機関はその管理者が他の取扱い操作で同じ違反を犯しているのを発見しました。

この場合、監督機関が課すことができる罰金の最高額はいくらですか？

A) 750ユーロ
B) 1,230,000ユーロ
C) 10,000,000ユーロ、またはその企業の全世界年間売上高の2%のいずれか高い方
D) 20,000,000ユーロ、または、最低額を20,000,000ユーロとするその企業の全世界年間売上高の4%のいずれか高い方

20 / 40
監督機関は、データ保護規則の順守を確保することを目的とした多数の責任を割り当てられています。

監督機関の責任に含まれているのはどれですか？

A) 個人データの取扱いに関連する特定の部門の行動規範を評価する
B) 個人データを保護するために実施すべき対策の最小のセットを定義する
C) 通知されたデータ侵害をすべて調査する
D) 規則のコンプライアンスについて契約と拘束的企業準則(BCR)をレビューする

21 / 40
ある宗教団体は、関係国の政府からの法的要件に順守するために、非ヨーロッパ諸国の宗教機関と個人データを共有したいと考えています。

このケースに適用されるGDPRの規則はどれですか？

A) 例外として、宗教的信条を開示する機微データの取扱いは宗教団体に許可される
B) 第三国からの法的要件に応じて、欧州経済領域（EEA）外に個人データを移転するのは適法ではない
C) データ主体から具体的かつ明確な同意が得られていれば取扱いは適法である
D) EU委員会が考案したモデル契約条項を使えば欧州経済領域（EEA）外での個人データの取扱いは許可される

22 / 40
2016年7月12日、欧州委員会は米国との間の個人データ移転に関する規則(EU-米国間プライバシーシールド）を発効しました。

GDPR用語では、この規則はどのような種類ですか？

A) 十分性の決定
B) 例外の法令
C) 標準的な拘束的契約
D) GDPRに取って代わる条約

23 / 40
拘束的企業準則(BCR)は、組織がGDPR に準拠する管理上の負担を緩和する手段の一つです。

BCRはどのように役立ちますか？

A) BCRによって、組織は国外で関連する全ての当事者との契約を支持できるようになる
B) BCRによって、組織はEEA域外の第三者に個人データを取り扱わせることができるようになる
C) BCRによって、EU域内の各監督機関に個別に働きかける必要がなくなる
D) BCRがいったん承認されれば、組織は監督機関にデータ取扱い許可を求める必要がなくなる

24 / 40
契約者が個人データの取り扱いを委託する場合、当事者は書面による契約を締結します。この契約は、取扱いの対象事項及び持続期間、取扱いの性質及び目的、個人データの種類及びデータ主体の種類を定めます。

他にこの契約書で規定しなければならないのはどれですか？

A) 取扱者の説明責任（アカウンタビリティ）
B) データ侵害の通知義務
C) 取扱者は監督機関と協力しなければならないという義務
D) 管理者（コントローラ）の義務と権利

25 / 40
管理者（コントローラ）が個人データの取扱いを取扱者に委託するには何をする必要がありますか？

A) 管理者は、データの取扱いを委託する許可を監督機関に申請する必要がある
B) 管理者は、合意された契約書が規則に適合しているかを監督機関に確認する必要がある
C) 管理者と取扱者は、データの機密性を保証する契約書を起草して署名する必要がある
D) 取扱者は、サービスレベル合意書(SLA)で合意された需要が全て満たされていることを管理者に示す必要がある

26 / 40
GDPRの第25条に規定されたデータ保護バイデザインは、7つの原則に基づいています。そのうち1つは通常*「全機能的ーゼロサムではなくポジティブサム」*と呼ばれます。

この原則の主旨は何ですか？

A) 適用されたセキュリティ基準によって個人データはそのライフサイクルを通じて機密性、完全性、可用性を保証されなければならない
B) 異なる種類の正当な目的が相反する場合、プライバシーの目的は他のセキュリティの目的よりも優先されなければならない
C) 提供された技術、プロセス、システムにプライバシーを組み込む場合、全面的な機能性を阻害しない方法で実施しなければならない
D) 可能な限り、詳細なプライバシーへの影響とリスク評価を実施して、プライバシーへのリスクを明確に文書化して公表するべきである

27 / 40
多くの場合、個人データを扱う仕事のスタッフはプライバシーと情報セキュリティを別々の問題として扱います。

このことが間違っている理由は何ですか？

A) 適切な情報セキュリティの対策を識別し、実施し、監視しなければ、プライバシーは保証されないため
B) 監督機関は、データ保護責任者と情報セキュリティ責任者の役割が統合されることを期待しているため
C) 規則によって、個人データの取扱いが許可される前に実施する必要のある特定の情報セキュリティの対策が識別されるため

28 / 40
データ保護影響評価(DPIA)の目的の一つは、「個人データが取り扱われ、プライバシーが尊重される方法について顧客または市民の信頼性を向上させる」ことです。

どのようにしてDPIAは「信頼性を向上させる」ことができますか？

A) 組織は、費用のかさむプロセス調整や後でシステムの再設計を行うリスクを最小限にできる
B) 組織はGDPRへの不適合を防止し、制裁金を科されるリスクを最小限にする
C) 組織は、プライバシーを重視しており、GDPRへのコンプライアンスを目指していることを証明する

29 / 40
監督機関によるデータ保護の監査の目的は何ですか？

A) GDPRに規定された、データ保護のために適切な技術的及び組織的な対策を実施する義務を履行すること
B) GDPRに従って取扱いが実施されていることを評価して、GDPRの適用を監視し、施行すること
C) GDPRへの不適合に対する賠償請求から管理者（コントローラ）を保護するため、プライバシーのリスクを軽減するよう管理者に助言すること

30 / 40
データの最小化の原則の**最適な**説明はどれですか？

A) データ主体のプライバシーと利益を守るため、可能な限り最小限のデータを収集するように注意すべきである
B) データは、取り扱われる目的の必要性に照らして、適切であり、関連性があり、最小限に限られていなければならない
C) データを管理できるようにしておくため、必要なストレージが最小限となるようにデータを格納すべきである
D) データ主体ごとに収集する項目数は、監督機関に規定された上限値を超えてはならない

31 / 40
セッションクッキーは最も一般的なクッキーの種類の一つです。

セッションクッキーについて、**最適な**説明はどれですか？

A) セッションクッキーは、ウェブ上での動作、例えば、ウェブショップで実際に注文をする前に選んだ商品などの情報を含んでいる
B) セッションクッキーは、ブラウザの履歴を開示するため、ウェブサイト側はそこへ行く前にアクセスした他のウェブサイトを知ることができる
C) セッションクッキーは、ブラウザの履歴を保存するため、そうしたければ、過去にアクセスしたウェブサイトをたどって同じサイトに行くことができる
D) セッションクッキーは、個人データを収集するため、ユーザが過去にアクセスしたウェブサイトに戻った時にそのユーザ名に対して挨拶したり過去の設定を再利用したりすることができる

32 / 40
ウェブサイトがマーケティング目的で訪問者を追跡してその情報を保存することがあります。

ウェブサイトには訪問者の情報がマーケティング目的に使用されることを訪問者に通知する義務がありますか？

A) ある
B) ない

33 / 40
ソーシャルメディアを活用して、ある会社が特定の分野で専門知識を持つ専門家であることを宣伝することができます。

特定分野での専門知識を実証するのに**最適な**方法はどれですか？

A) ソーシャルメディアに会社の情報を投稿する
B) ソーシャルメディア上で自社製品に関する質問に積極的に回答する
C) 競合他社の製品が自社製品と比べてどう劣っているかを投稿する
D) 自社が開発中の新製品について投稿する

34 / 40
個人データも保管されている情報システム内でセキュリティ侵害が発生しました。

管理者（コントローラ）が**最初に**すべきことは何ですか？

A) 侵害によって個人データの喪失または違法な取扱いが起きた可能性があるかを確認する
B) データ保護影響評価(DPIA)を利用してデータ主体に悪影響が起きるリスクを評価する
C) 機微な性質の個人データに違法な取扱いがされたか、または、された可能性があるかを評価する
D) 関係監督機関に迅速に侵害を報告する

35 / 40
「プライバシー」という用語はGDPRでは言及されていません。

「プライバシー」は「データ保護」とどのように関連しますか？

A) データ保護とは、個人データの処理に関する一連の規則と規制である。プライバシーはデータ保護の結果である。
B) プライバシーは、個人的な問題への干渉から保護される権利である。データ保護は、その保護を実装する手段である。
C) プライバシーは個人的な事柄を秘密にしておく権利である。データ保護は個人データを秘密にしておく権利である。
D) 「プライバシー」と「データ保護」という用語は同じ意味を持つ。意味に実質的な違いはない。

36 / 40
GDPRとして知られる規則(EU) 2016/679は、以前発行されたEU指令を置き換えるものです。

無効にされる（置き換えられる）のはどの指令ですか？

A) 2002年7月12日の指令2002/58/EC
B) 2006年3月15日の指令2006/24/EC
C) 1995年10月24日の指令95/46/EC
D) 1997年12月15日の指令97/66/EC

37 / 40
GDPRで明確に定義されているデータ主体の権利はどれですか？

A) 個人データのコピーは、データ主体の要求する形式で提供されなければならない
B) データ主体の費用は一切なしで個人データにアクセスできること
C) データ主体の依頼があればいつでも個人データは変更されなければならない
D) データ主体の依頼があればいつでも個人データは消去されなければならない

38 / 40
GDPRは「機微な個人データ」を特別な種類の個人データとして区別しています。

そのようなデータの例はどれですか？

A) 病院の専門医の予約
B) 国際銀行番号(IBAN)
C) 政治学の学術雑誌の購読契約
D) 協会支部の会員資格

39 / 40
データ保護の役割のうち、個人データ取扱いの目的と手段を決定するのはどの役割ですか？

A) 管理者（コントローラ）
B) データ保護責任者(DPO)
C) 取扱者

40 / 40
GDPRにおいて個人データと見なされる情報はどれですか？

A) たとえ真実でなくても、その人のプライバシーを害する可能性のある人物に関する情報
B) 識別可能な自然人に関するあらゆる情報
C) 識別可能な自然人に関するデジタル化された情報

解答と解説

1 / 40
個人データの違法な収集、保存、改変、開示、拡散は、犯罪であると欧州の法律で規定されています。

この犯罪の種類はどれですか？

A) コンテンツ関連犯罪
B) 金融犯罪
C) 知的財産犯罪
D) プライバシー犯罪

A) 不正解。コンテンツ関連犯罪は、人種差別的声明、（児童）ポルノ、暴力を教唆する情報の拡散に関連するものです。
B) 不正解。金融犯罪は、システムへの不正なアクセス（ハッキング、ウィルス配布など）や、コンピュータを使用したスパイ行為、偽造及び詐欺に関連するものです。
C) 不正解。知的財産犯罪は、著作権や関連する権利の侵害に関連するものです。
D) 正解。個人データの違法な取扱いはすべて犯罪です。基本知識であり、ソースはありません。

2 / 40
プライバシーとデータ保護はどのように関連していますか？

A) データ保護はプライバシーの一部である
B) プライバシーはデータ保護の一部である
C) プライバシーとデータ保護は同じである
D) データ保護がなければプライバシーは保てない

A) 不正解。プライバシーの概念は、空間的、関係的、身体的、情報的など多岐にわたります。データ保護が関連を持たない概念もあります。
B) 不正解。プライバシーの概念は、空間的、関係的、身体的、情報的など多岐にわたります。データ保護が保証に役立つ概念もあります。
C) 不正解。例えば、空間的プライバシーにはデータ保護は関連しません。
D) 正解。データ保護は、プライバシーに対する基本的な権利を保護するために必要な対策です。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - §1.3 定義。

3 / 40
GDPRの主な目的は何ですか？

A) EU加盟国が自国の法律を制定するための基盤となること
B) EU域内の個人のプライバシーの権利を非EU加盟国に尊重させること
C) プライバシーを誰もが持つ基本的人権として確保すること
D) EU域内の個人のデータ保護を強化して統一すること

A) 不正解。GDPRは規則であるため、EU加盟国のデータ保護法を無効にします。
B) 不正解。GDPRの主な目的はEU域内の個人のデータ保護の権利を定義することを目指しています。
C) 不正解。GDPRはデータ保護は基本的人権であるとは明確に記述していません。また、その範囲はEU域内の個人に限られています。
D) 正解。GDPRの適用範囲は、EU域内の個人の権利としてのデータ保護に限られており、EU域内の規則の統一を目指しています。ソース：EU GDPR、ポケットガイド- 序章。

4 / 40
GDPRは個人データの保護に関連します。

個人データの定義は何ですか？

A) 識別された、または識別可能な自然人に関連するあらゆる情報
B) EU市民が保護したいと思うあらゆる情報
C) 人種や民族背景、宗教的見解、健康や性的習慣に関するデータを直接的または間接的に明らかにするデータ
D) 情報の機密性、完全性、可用性の維持

A) 正解。これはデータ保護の公式な定義です。ソース：EU GDPR、ポケットガイド - 第2章　用語と定義GDPR 2016/679 第4条：定義
B) 不正解。この定義は一般的すぎます。
C) 不正解。これは機微データの定義であり、一般的な個人データの定義ではありません。
D) 不正解。これはISO/IEC 27000:2014に規定された情報セキュリティの定義です。

5 / 40
GDPRによると、機微データに分類される個人データはどれですか？

A) クレジットカードの詳細
B) 労働組合員資格
C) パスポート番号
D) 社会保障番号

A) 不正解。クレジットカードの詳細はGDPRで規定された機微データではありません。
B) 正解。労働組合員資格は機微データです。ソース：GDPR 第9条　詳述部10　特別な種類の個人データ
C) 不正解。パスポートの詳細はGDPRで規定された機微データではありません。
D) 不正解。社会保障番号はGDPRで規定された機微データではありません。

6 / 40
GDPRに規定された個人データの「取扱（処理）」の定義は何ですか？

A) 個人データに対して実施できるすべての操作
B) 個人データに対して実施できる、消去と破棄以外のすべての操作
C) データをソーシャルメディアで共有する操作、もしくは、データをメール添付またはインターネット経由で送付する操作のみ
D) 個人データを収集した目的のために使用する操作のみ

A) 正解。ソース：GDPR 第4条(2)
B) 不正解。「取扱（処理）」は、個人データに対して実施するあらゆる操作を意味します。
C) 不正解。「取扱（処理）」は、個人データに対して実施するあらゆる操作を意味します。
D) 不正解。「取扱（処理）」は、個人データに対して実施するあらゆる操作を意味します。

7 / 40
「*第51条の規定に基づいて加盟国により設立された独立した公共機関*」

これはデータ保護におけるどの役割の定義ですか？

A) 管理者（コントローラ）
B) 取扱者
C) 監督機関
D) 第三者

A) 不正解。規則2016/679の第4条を参照してください。
B) 不正解。規則2016/679の第4条を参照してください。
C) 正解。ソース：規則2016/679の第4条及び第51条。
D) 不正解。規則2016/679の第4条を参照してください。

8 / 40
GDPRでは、告知に基づく同意（インフォームドコンセント）は個人データを取扱うための適法的根拠です。同意を得た取扱い目的は文書化する必要があります。

データ主体の同意を得なければならないのは、個人データを取扱う場合のどの段階ですか？

A) 取扱い目的の詳細が示された後で、かつ個人データを収集する前
B) 取扱い目的の詳細が作成されて表示される前
C) 個人データを取扱う前
D) 個人データが公表されるかまたは拡散される前

A) 正解。同意は目的の詳細がデータ主体に提示された後にのみ得ることができます。ソース：GDPR詳述部(32)、(42)。
B) 不正解。同意は目的の詳細がデータ主体に提示された後にのみ得ることができます。
C) 不正解。個人データの収集は「取扱い」に該当するため、それ自体に告知に基づく同意をデータ主体から得なければなりません。
D) 不正解。個人データの公表および拡散は「取扱い」に該当するため、それ自体に告知に基づく同意をデータ主体から得なければなりません。

9 / 40
GDPRは比例性と補完性の原理を基礎としています。

この文脈での「比例性」の意味は何ですか？

A) 個人データは目的の仕様に従ってのみ取扱いが可能である
B) 個人データは、明示的かつ告知に基づく同意がなければ再利用してはならない
C) 個人データは、他に目的を達成する手段がない場合にのみ取扱うことが可能である
D) 個人データは、目的に照らして適切であり、関連性があり、過度であってはならない

A) 不正解。これは法的制限の1つです。
B) 不正解。これは法的制限の1つです。
C) 不正解。これは補完性の定義です。
D) 正解。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - § 3.1.2 比例性と補完性、及びGDPR第35条(7)。

10 / 40
個人データの取扱いは一定の品質要件を満たさなければなりません。

GDPRが定義する品質要件に含まれるのはどれですか？

A) 取扱ったデータはアーカイブに入れなければならない
B) 取扱ったデータは暗号化しなければならない
C) 取扱ったデータは索引付けしなければならない
D) 取扱ったデータは関連付けしていなければならない

A) 不正解。このような要件はGDPRには定義されていません。
B) 不正解。このような要件はGDPRには定義されていません。
C) 不正解。このような要件はGDPRには定義されていません。
D) 正解。この要件はGDPRに定義されています。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - § 3.1.2 比例性と補完性。

11 / 40
個人データを取り扱う場合は常に比例性と補完性を確認する必要があります。

取り扱い中の個人データの要件はどれですか？

A) 定義された目標の達成に必要なものに常に限定する必要があり、また、「干渉性」が最低限のデータに制限する必要がある
B) 可能な限り少人数の従業員が取扱わなければならず、また、取り扱う従業員は管理者（コントローラ）または提携会社の下で作業しなければならない
C) あらかじめ決められたストレージサイズに限定する必要があり、使用するシステムは管理者（コントローラ）が資金調達をする必要がある
D) 可能な限り少数の目的に使用しなければならず、また、取扱者の敷地外では使用してはならない

A) 正解。比例性と補完性とは、定義済みの目標を達成するのに必要な量以上のデータは収集しないこと、また、データ主体のプライバシーに最小限の影響を及ぼすデータを使うように常に努めることを意味します。ソース：GDPR、ポケットガイド - 第3章、規則 - 適法な取扱い。
B) 不正解。従業員の数や子会社への提携はこれらの用語に関係がありません。
C) 不正解。ストレージサイズやシステムの資金調達者はこれらの用語に関係がありません。
D) 不正解。データ主体が同意する限り、目標の数は明確に制限されず、また、場所も制限されません。

12 / 40
「管理者（コントローラ）は、（略）各具体的取扱いの目的に必要な個人データのみが取り扱われることを保証するための適切な技術的及び組織的対策を実施しなければならない。」

これはGDPRのどの用語の定義ですか？

A) コンプライアンス
B) データ保護バイデフォルト
C) データ保護バイデザイン
D) 組込保護

A) 不正解。コンプライアンスとは、規則や基準に適合または合格した状態や事実です。
B) 正解。デフォルトで、最小限の個人データを、不正アクセスを防止するための最善のセキュリティ手段を使って、可能な限り最短の期間で取り扱わなくてはなりません。ソース：EU GDPR、ポケットガイド - 第3章　規則 - データ保護バイデザイン及びデータ保護バイデフォルト、GDPR 第20条（2）。
C) 不正解。データ保護バイデザインとは、データ保護の原則を実施する適切な手段を含むデザインを指します。
D) 不正解。組込データ保護はデータ保護バイデザインの結果です。

13 / 40
GDPRでは、個人データの不正な開示や個人データへの不正アクセスはどのように呼ばれますか？

A) 機密性侵害
B) データ侵害
C) インシデント
D) セキュリティ　インシデント

A) 不正解。GDPRでは「データ侵害」と呼びます。データ侵害は必ずしも機密性侵害ではありません。
B) 正解。ソース：EU GDPR、ポケットガイド - 第3章　規則 - データ侵害、GDPR 第4条 (12)。
C) 不正解。GDPRでは「データ侵害」と呼びます。インシデントは必ずしもデータ侵害ではありません。
D) 不正解。GDPRでは「データ侵害」と呼びます。セキュリティ侵害は必ずしもデータ侵害ではありません。

14 / 40
機微な個人データのデータ侵害が発生したことが確認されました。

GDPRによると、このデータ侵害は最終的に誰に報告をする必要がありますか？

A) 監督機関
B) データ保護責任者(DPO)
C) その部門のマネージャ
D) 警察

A) 正解。データ侵害がデータ主体やその個人データのセキュリティに重大な影響を与える可能性がある場合、データ保護機関(DPA)に報告する必要があります。ソース：EU GDPR、ポケットガイド - 第 3 章　規則　データ侵害、GDPR 第4条 (12)。
B) 不正解。内部のデータ保護責任者(DPO)に報告するかもしれませんが、最終的にはデータ保護機関(DPA)に報告しなければなりません。
C) 不正解。その部門のマネージャに報告するかもしれませんが、最終的にはデータ保護機関(DPA)に報告しなければなりません。
D) 不正解。データ侵害は必ずしも警察に報告する必要はありませんが、最終的にはデータ保護機関(DPA)に報告しなければなりません。

15 / 40
バックアップの実行中にデータサーバのディスクがクラッシュしました。データとバックアップの両方が失われました。ディスクには個人データが含まれていましたが、機微データはありませんでした。

このインシデントの種類は何ですか？

A) データ侵害
B) セキュリティ侵害
C) セキュリティ　インシデント

A) 正解。回復不能な方法で失われた個人データは不正な取扱いとみなされ、データ侵害を構成します。ソース：EU GDPR、ポケットガイド -第3 章　規則 - データ侵害、 GDPR I章 第4条定義。
B) 不正解。回復不能な方法で失われた個人データは不正な取扱いとみなされ、データ侵害を構成します。
C) 不正解。回復不能な方法で失われた個人データは不正な取扱いとみなされ、データ侵害を構成します。

16 / 40
労働組合のある従業員が、組合員宅に送付するニュースレターのドラフトを完成させるために自宅に持ち帰りました。ドラフトと送付先リストを入れたUSBスティックを紛失しました。

このデータ侵害は、特に誰に報告すべきですか？

A) 送付先リストに記載された組合員全員
B) 労働組合のスタッフ
C) 警察

A) 正解。これは機密データであるため、損失はプライバシー機関とデータ主体の両方に報告する必要があります。ソース：EU GDPR、ポケットガイド - 第3章　規則 - データ侵害。
B) 不正解。これは機微データであるため、紛失はプライバシー機関とデータ主体の両方に報告する必要があります。
C) 不正解。これは機微データであるため、紛失はプライバシー機関とデータ主体の両方に報告する必要があります。

17 / 40
あるソーシャルサービス組織は、クライアントを管理するための新しいデータベースを設計し、必要な配慮（診療）を計画しています。

監督機関に許可を申請するためにとるべき最初の重要なステップに含まれるのはどれですか？

A) クライアントに関するデータ、また、必要かつ提供される配慮（ケア）の量と種類に関するデータを収集する
B) データ保護影響評価(DPIA)を実施して、意図する取扱いのリスクを評価する
C) 個人データの意図する取扱いについて、クライアントの同意を得る

A) 不正解。医療に関わる個人データの収集は、定義によれば「機微データの取扱い」です。事前にデータ保護機関(DPA)とデータ主体から許可を得る必要があります。
B) 正解。データ取扱いの同意を依頼する際、データ主体は「リスク、規則、保護措置および権利（略）について認識していなければなりません」。ソース：EU GDPR、ポケットガイド - 第3章　規則 - 同意 、GDPR 詳述部（39）。
C) 不正解。データ取扱いの同意を依頼する際、データ主体は「リスク、規則、保護措置および権利（略）について認識していなければなりません」。これらのリスクや保護措置を評価するには最初にDPIAが必要です。

18 / 40
データ主体が常にデータ侵害の通知を受ける必要があるのはどのような場合ですか？

A) EU域内に所在しない取扱者の施設で個人データが取扱われた場合
B) 個人データは、管理者（コントローラ）が送信した取扱契約書の草案に同意した当事者によって取扱われたが、まだ署名していない場合
C) 個人データが取扱われたシステムが攻撃され、ストレージ装置が損傷した場合
D) 侵害がデータ主体のプライバシーに有害な結果をもたらす重大な可能性がある場合

A) 不正解。データが取扱われた場所は、データ主体に対するデータ侵害の通知義務には特に重要な意味を持ちません。
B) 不正解。有効な書面による契約なしに管理者（コントローラ）以外の者が処理した個人データは、データ侵害とみなされます。しかしながら、与えられた状況下では、データ主体にとって否定的な結果は起こりそうもない。その場合、データ主体への通知は必須ではありません。
C) 不正解。ストレージ装置の損害により、データへのアクセスが困難または不可能になることもありますが、不正な取扱を意味するものではありません
D) 正解。データ主体に悪影響を与える可能性が高い場合、管理者（コントローラ）は侵害を通知する義務があります。。ソース：ホワイトペーパー- プライバシー、個人データ及びGDPR - § 5.2データ侵害発生時の対応手順

19 / 40
あるオランダの管理者（コントローラ）は、監督機関に相談せずに、北アフリカの国の取扱者に機微な個人データの取扱いを委託していました。これが発覚し、管理者は監督機関から処罰を受けました。6か月後、監督機関はその管理者が他の取扱い操作で同じ違反を犯しているのを発見しました。

この場合、監督機関が課すことができる罰金の最高額はいくらですか？

A) 750ユーロ
B) 1,230,000ユーロ
C) 10,000,000ユーロ、またはその企業の全世界年間売上高の2%のいずれか高い方
D) 20,000,000ユーロ、または、最低額を20,000,000ユーロとするその企業の全世界年間売上高の4%のいずれか高い方

A) 不正解。GDPR第83条第3項によると、制裁金の最高金額は、最低額を20,000,000ユーロとするその企業の全世界年間売上高の4%です。
B) 不正解。GDPR第83条第3項によると、制裁金の最高金額は、最低額を20,000,000ユーロとするその企業の全世界年間売上高の4%です。
C) 不正解。GDPR第83条第3項によると、制裁金の最高金額は、最低額を20,000,000ユーロとするその企業の全世界年間売上高の4%です。
D) 正解。これは違反に対する最上限です。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - §7.3.3過料（制裁金）を課す一般条件。

20 / 40
監督機関は、データ保護規則の順守を確保することを目的とした多数の責任を割り当てられています。

監督機関の責任に含まれているのはどれですか？

A) 個人データの取扱いに関連する特定の部門の行動規範を評価する
B) 個人データを保護するために実施すべき対策の最小のセットを定義する
C) 通知されたデータ侵害をすべて調査する
D) 規則のコンプライアンスについて契約と拘束的企業準則(BCR)をレビューする

A) 正解。規則を遵守する方法について全般的な助言をすることはデータ保護機関(DPA)の役割の1つです。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - §7.1.4基準の設定方法。
B) 不正解。データ保護機関(DPA)は、セキュリティの適切なレベルであるとみなされるものについて全般的な助言を行います。しかし、そのレベルを実現するのにとるべき特定の対策について教えることはありません。DPAが望んだとしても特定の対策を教えることはできません。どの組織にも応用できる万能の対策はないからです。
C) 不正解。データ保護機関(DPA)には通知されたデータ侵害をすべて調査する義務はなく、調査するキャパシティもありません。しかし、DPAが重大または注目すべきと見なしたものは調査されます。
D) 不正解。データ保護機関(DPA)は法律顧問ではないため、契約と拘束的企業準則(BCR)をレビューすることはありません。しかし、調査中に特定の契約や一連のBCRに目を通す可能性はあります。

21 / 40
ある宗教団体は、関係国の政府からの法的要件に順守するために、非ヨーロッパ諸国の宗教機関と個人データを共有したいと考えています。

このケースに適用されるGDPRの規則はどれですか？

A) 例外として、宗教的信条を開示する機微データの取扱いは宗教団体に許可される
B) 第三国からの法的要件に応じて、欧州経済領域（EEA）外に個人データを移転するのは適法ではない
C) データ主体から具体的かつ明確な同意が得られていれば取扱いは適法である
D) EU委員会が考案したモデル契約条項を使えば欧州経済領域（EEA）外での個人データの取扱いは許可される

A) 不正解。宗教団体は、過去及び現在の信者の個人データの取扱いを認められていますが、*第三国からの法的要件に応じてEEA域外に個人データを移転するのは適法ではありません。*
B) 正解。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - §7.5.2 EEA域外へのデータ移転に適用される規則、EU GDPR、ポケットガイド - 第3章：規則 - 国際移転、GDPR第48条。
C) 不正解。第三国からの法的要件に応じてEEA域外に個人データを移転するのは適法ではありません。*たとえデータ主体の同意があったとしても適法とはなりません。*
D) 不正解。EU域外での機微データの取扱いは適法である場合もありますが、第三国からの法的要件に応じる場合には適法ではありません。

22 / 40
2016年7月12日、欧州委員会は米国との間の個人データ移転に関する規則(EU-米国間プライバシーシールド）を発効しました。

GDPR用語では、この規則はどのような種類ですか？

A) 十分性の決定
B) 例外の法令
C) 標準的な拘束的契約
D) GDPRに取って代わる条約

A) 正解。この規則は、第三国での取扱いに関してGDPRに準拠した十分性の決定です。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - §7.5.4 EEAと米国間のデータ移転に適用される規則、EU GDPR、ポケットガイド - 第3章 規則 - 国際移転、GDPR詳述部104及び106。
B) 不正解。例外は、テロ攻撃や重大犯罪に対応するのに必要となる移転に関連するものです。（第11条）
C) 不正解。この規則は、第三国での取扱いに関してGDPRに準拠した十分性の決定です。
D) 不正解。この規則は、第三国での取扱いに関してGDPRに準拠した十分性の決定です。

23 / 40
拘束的企業準則(BCR)は、組織がGDPR に準拠する管理上の負担を緩和する手段の一つです。

BCRはどのように役立ちますか？

A) BCRによって、組織は国外で関連する全ての当事者との契約を支持できるようになる
B) BCRによって、組織はEEA域外の第三者に個人データを取り扱わせることができるようになる
C) BCRによって、EU域内の各監督機関に個別に働きかける必要がなくなる
D) BCRがいったん承認されれば、組織は監督機関にデータ取扱い許可を求める必要がなくなる

A) 不正解。BCRは起草されているので、組織は書面による基盤契約を提携会社ごとに使う必要はありません。
B) 不正解。BCRは、組織とその提携会社すべてとの間でのみ有効です。他の関係者には適用されません。
C) 正解。いったんEU域内の一つのデータ保護機関(DPA)でBCRが承認されれば、EU域内の他のDPAに同じBCRの承認を申請する必要がなくなります。ソース：EU GDPR、ポケットガイド -第3章　規則 - 拘束的企業準則(BCR)。
D) 不正解。BCRはDPAからも承認を受ける必要があります。

24 / 40
契約者が個人データの取り扱いを委託する場合、当事者は書面による契約を締結します。この契約は、取扱いの対象事項及び持続期間、取扱いの性質及び目的、個人データの種類及びデータ主体の種類を定めます。

他にこの契約書で規定しなければならないのはどれですか？

A) 取扱者の説明責任（アカウンタビリティ）
B) データ侵害の通知義務
C) 取扱者は監督機関と協力しなければならないという義務
D) 管理者（コントローラ）の義務と権利

A) 不正解。これは取扱者に課されるGDPRの直接義務です。
B) 不正解。これは取扱者に課されるGDPRの直接義務です。
C) 不正解。これは取扱者に課されるGDPRの直接義務です。
D) 正解。これは取扱者に課されるGDPRの直接義務です。ソース：EU GDPR、ポケットガイド - 第3章 規則 - 管理者／取扱者の契約、GDPR第28条 (3)。

25 / 40
管理者（コントローラ）が個人データの取扱いを取扱者に委託するには何をする必要がありますか？

A) 管理者は、データの取扱いを委託する許可を監督機関に申請する必要がある
B) 管理者は、合意された契約書が規則に適合しているかを監督機関に確認する必要がある
C) 管理者と取扱者は、データの機密性を保証する契約書を起草して署名する必要がある
D) 取扱者は、サービスレベル合意書(SLA)で合意された需要が全て満たされていることを管理者に示す必要がある

A) 不正解。委託案件ごとにデータ保護機関(DPA)に許可を申請する必要はありません。
B) 不正解。データ保護機関(DPA)は法律顧問ではないため、契約書に関するコンプライアンスの側面を確認することはありません。
C) 正解。管理者が取扱い目的と取扱い手段を定義した、データの機密性を保証する契約書が必要です。管理者と取扱者はこの契約書を締結しなければなりません。ソース：EU GDPR、ポケットガイド - 第3章 規則 - 管理者／取扱者の契約、GDPR第28条 (3)。
D) 不正解。SLAは運用の側面を重視しており、目的の定義をするとは限らないため、不十分です。

26 / 40
GDPRの第25条に規定されたデータ保護バイデザインは、7つの原則に基づいています。そのうち1つは通常*「全機能的ーゼロサムではなくポジティブサム」*と呼ばれます。

この原則の主旨は何ですか？

A) 適用されたセキュリティ基準によって個人データはそのライフサイクルを通じて機密性、完全性、可用性を保証されなければならない
B) 異なる種類の正当な目的が相反する場合、プライバシーの目的は他のセキュリティの目的よりも優先されなければならない
C) 提供された技術、プロセス、システムにプライバシーを組み込む場合、全面的な機能性を阻害しない方法で実施しなければならない
D) 可能な限り、詳細なプライバシーへの影響とリスク評価を実施して、プライバシーへのリスクを明確に文書化して公表するべきである

A) 不正解。これは残り6つの原則のひとつ、「エンドツーエンドセキュリティーライフサイクル保護」の側面です。
B) 不正解。データ保護バイデザインでは、プライバシーが他の正当な利益やデザイン目標、技術的能力と競合するアプローチを却下しています。全ての目標はポジティブサムな「ウィンウィン」な方式で共存しなければなりません。
C) 正解。これが主旨です。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - § 8.1.1データ保護バイデザインの7つの原則、GDPR第25条。
D) 不正解。これは残り6つの原則のひとつ、「プライバシー*組込*デザイン」の側面です。

27 / 40
多くの場合、個人データを扱う仕事のスタッフはプライバシーと情報セキュリティを別々の問題として扱います。

このことが間違っている理由は何ですか？

A) 適切な情報セキュリティの対策を識別し、実施し、監視しなければ、プライバシーは保証されないため
B) 監督機関は、データ保護責任者と情報セキュリティ責任者の役割が統合されることを期待しているため
C) 規則によって、個人データの取扱いが許可される前に実施する必要のある特定の情報セキュリティの対策が識別されるため

A) 正解。プライバシーとデータ保護の目的は、個人データなどの機密性を保証することです。これにはセキュリティ対策の実施が必要とされます。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - § 2.1.6 - 完全性と機密性。
B) 不正解。データ保護機関(DPA)はこれらの役割を統合することを全く期待していません。
C) 不正解。規則は達成すべき目標を特定しますが、実施すべき特定の対策は示しません。

28 / 40
データ保護影響評価(DPIA)の目的の一つは、「個人データが取り扱われ、プライバシーが尊重される方法について顧客または市民の信頼性を向上させる」ことです。

どのようにしてDPIAは「信頼性を向上させる」ことができますか？

A) 組織は、費用のかさむプロセス調整や後でシステムの再設計を行うリスクを最小限にできる
B) 組織はGDPRへの不適合を防止し、制裁金を科されるリスクを最小限にする
C) 組織は、プライバシーを重視しており、GDPRへのコンプライアンスを目指していることを証明する

A) 不正解。この側面は経営陣の信頼を高めるかもしれませんが、顧客または市民の信頼は高めません。
B) 不正解。制裁金の防止は経営陣の信頼を高めるかもしれませんが、顧客または市民の信頼は高めません。
C) 正解。ソース：EU GDPR、ポケットガイド - 第3章　規則 - データ保護の影響評価

29 / 40
監督機関によるデータ保護の監査の目的は何ですか？

A) GDPRに規定された、データ保護のために適切な技術的及び組織的な対策を実施する義務を履行すること
B) GDPRに従って取扱いが実施されていることを評価して、GDPRの適用を監視し、施行すること
C) GDPRへの不適合に対する賠償請求から管理者（コントローラ）を保護するため、プライバシーのリスクを軽減するよう管理者に助言すること

A) 不正解。データ保護の監査は対策の実施ではなく、対策の効果を評価するものです。
B) 正解。GDPRによると、これは監督機関としてのデータ保護機関(DPA)の重要な役割です。ソース：GDPR 第57条1(a)。
C) 不正解。データ保護機関(DPA)はコンプライアンスを監視し、改善について助言をする役割を担いますが、その目的は管理者を保護することではありません。

30 / 40
データの最小化の原則の**最適な**説明はどれですか？

A) データ主体のプライバシーと利益を守るため、可能な限り最小限のデータを収集するように注意すべきである
B) データは、取り扱われる目的の必要性に照らして、適切であり、関連性があり、最小限に限られていなければならない
C) データを管理できるようにしておくため、必要なストレージが最小限となるようにデータを格納すべきである
D) データ主体ごとに収集する項目数は、監督機関に規定された上限値を超えてはならない

A) 不正解。実際にはGDPRは収集するデータは適切でなければならないと規定しており、絶対的な最小限である必要はありません。
B) 正解。これがデータの最小化の定義そのものです。これは、定義された目的の実行に必要なデータのみが収集されるのを確実にすることを目指しています。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - §2.1 データ取扱いの原則、GDPR第5条1.c。
C) 不正解。ストレージのサイズはこの原則に関係がありません。
D) 不正解。データ保護機関(DPA)は、データが定義された目的の実行に必要なものに限定されている限り、収集する項目数に上限値を設定しません。

31 / 40
セッションクッキーは最も一般的なクッキーの種類の一つです。

セッションクッキーについて、**最適な**説明はどれですか？

A) セッションクッキーは、ウェブ上での動作、例えば、ウェブショップで実際に注文をする前に選んだ商品などの情報を含んでいる
B) セッションクッキーは、ブラウザの履歴を開示するため、ウェブサイト側はそこへ行く前にアクセスした他のウェブサイトを知ることができる
C) セッションクッキーは、ブラウザの履歴を保存するため、そうしたければ、過去にアクセスしたウェブサイトをたどって同じサイトに行くことができる
D) セッションクッキーは、個人データを収集するため、ユーザが過去にアクセスしたウェブサイトに戻った時にそのユーザ名に対して挨拶したり過去の設定を再利用したりすることができる

A) 正解。セッションクッキーは、そのセッションの情報をメモリに保存します。セッションを閉じるとその情報は消去されます。ソース：ホワイトペーパー - プライバシー、個人データ及びGDPR - §8.6.3 クッキー。
B) 不正解。セッションを閉じるとセッションクッキーは消去されるため、次のセッションでは使うことができません。
C) 不正解。セッションを閉じるとセッションクッキーは消去されるため、次のセッションでは使うことができません。
D) 不正解。セッションを閉じるとセッションクッキーは消去されるため、次のセッションでは使うことができません。

32 / 40
ウェブサイトがマーケティング目的で訪問者を追跡してその情報を保存することがあります。

ウェブサイトには訪問者の情報がマーケティング目的に使用されることを訪問者に通知する義務がありますか？

A) ある
B) ない

A) 正解。ウェブサイトには訪問者の情報がマーケティング目的に使用されることを訪問者に通知する義務があります。訪問者には、マーケティングの目的で彼または彼女に関する個人データの処理に異議を申し立てる権利があります。ソース：ホワイトペーパー -プライバシー、個人データ及びGDPR - § 8.6.3 クッキー。
B) 不正解。ウェブサイトには訪問者の情報がマーケティングの目的に使用されることを訪問者に通知する義務があります。訪問者には、マーケティングの目的で彼または彼女に関する個人データの処理に異議を申し立てる権利があります。

33 / 40
ソーシャルメディアを活用して、ある会社が特定の分野で専門知識を持つ専門家であることを宣伝することができます。

特定分野での専門知識を実証するのに**最適な**方法はどれですか？

A) ソーシャルメディアに会社の情報を投稿する
B) ソーシャルメディア上で自社製品に関する質問に積極的に回答する
C) 競合他社の製品が自社製品と比べてどう劣っているかを投稿する
D) 自社が開発中の新製品について投稿する

A) 不正解。会社の情報を投稿するだけではその分野の専門家にはなれません。
B) 正解。ソーシャルメディア上で特定の製品に関する質問に回答（しかも積極的に）することで会社が専門家の地位を獲得する可能性があります。ソース：ホワイトペーパー -プライバシー、個人データ及びGDPR - § 8.6.データ、マーケティング及びソーシャルメディアの利用に関連するプラクティス。
C) 不正解。これは自社製品がいかに優れているかを自慢するだけです（優れていないかもしれません）。
D) 不正解。これは会社が新製品を開発していることを知らせるだけにすぎず、売り上げ増につながる可能性もありますが、会社が専門家の地位を獲得する可能性はありません。

34 / 40
個人データも保管されている情報システム内でセキュリティ侵害が発生しました。

管理者（コントローラ）が**最初に**すべきことは何ですか？

A) 侵害によって個人データの喪失または違法な取扱いが起きた可能性があるかを確認する
B) データ保護影響評価(DPIA)を利用してデータ主体に悪影響が起きるリスクを評価する
C) 機微な性質の個人データに違法な取扱いがされたか、または、された可能性があるかを評価する
D) 関係監督機関に迅速に侵害を報告する

A) 正解。ソース：ホワイトペーパー -プライバシー、個人データ及びGDPR - § 5.2データ侵害発生時の対応手順。
B) 不正解。データ保護影響評価(DPIA)は、個人データ取扱い操作を設計する際に実施します。
C) 不正解。管理者（コントローラ）は、まず、このインシデントが報告が必要なデータ侵害かどうかを確認しなければなりません。
D) 不正解。管理者（コントローラ）は、まず、このインシデントが報告が必要なデータ侵害かどうかを確認しなければなりません。

35 / 40
「プライバシー」という用語はGDPRでは言及されていません。

「プライバシー」は「データ保護」とどのように関連しますか？

A) データ保護とは、個人データの処理に関する一連の規則と規制である。プライバシーはデータ保護の結果である。
B) プライバシーは、個人的な問題への干渉から保護される権利である。データ保護は、その保護を実装する手段である。
C) プライバシーは個人的な事柄を秘密にしておく権利である。データ保護は個人データを秘密にしておく権利である。
D) 「プライバシー」と「データ保護」という用語は同じ意味を持つ。意味に実質的な違いはない。

A) 不正解。プライバシーは権利、データ保護はそれを保証する手段である
B) 正解。ソース：ホワイトペーパー -プライバシー、個人データ及びGDPR - § 1.3 定義
C) 不正解。プライバシーは権利、データ保護はそれを保証する手段である
D) 不正解。プライバシーは権利、データ保護はそれを保証する手段である

36 / 40
GDPRとして知られる規則(EU) 2016/679は、以前発行されたEU指令を置き換えるものです。

無効にされる（置き換えられる）のはどの指令ですか？

A) 2002年7月12日の指令2002/58/EC
B) 2006年3月15日の指令2006/24/EC
C) 1995年10月24日の指令95/46/EC
D) 1997年12月15日の指令97/66/EC

A) 不正解。指令2002/58/ECは、97/66/ECの一部を改正しました。
B) 不正解。この指令は、インターネットプロバイダによってインスタンスごとに収集されたデータの保持に関連するものです。
C) 正解。この置き換えは規則の副題で言及されています。ソース：GDPR
D) 不正解。この指令は、EU加盟国における基本的人権と自由の保護の平等なレベルを確保するために95/46/ECを補完するものです。

37 / 40
GDPRで明確に定義されているデータ主体の権利はどれですか？

A) 個人データのコピーは、データ主体の要求する形式で提供されなければならない
B) データ主体の費用は一切なしで個人データにアクセスできること
C) データ主体の依頼があればいつでも個人データは変更されなければならない
D) データ主体の依頼があればいつでも個人データは消去されなければならない

A) 不正解。個人データは、構造化され、一般的に利用され機械可読性のある形式で提供されなければなりませんが、必ずしもデータ主体の指定する形式である必要はありません。
B) 正解。しかし、無料で提供されなければならないのは最初の1部のみです。ソース：EU GDPR、ポケットガイド - 第3章　規則- データ主体の権利。
C) 不正解。誤ったデータのみが修正されなければなりません。
D) 不正解。第17条は、法的主張の立証、行使若しくは抗弁のためにデータが必要な場合などの例外を規定しています。

38 / 40
GDPRは「機微な個人データ」を特別な種類の個人データとして区別しています。

そのようなデータの例はどれですか？

A) 病院の専門医の予約
B) 国際銀行番号(IBAN)
C) 政治学の学術雑誌の購読契約
D) 協会支部の会員資格

A) 正解。病院の専門医の予約は「健康に関する個人データ」です。GDPR第9条1を参照してください。
B) 不正解。国際銀行番号(IBAN)は一意に個人に関連するデータ、すなわち個人データですが、GDPR第9条に規定された機微な個人データではありません。
C) 不正解。政治学の学術雑誌の購読契約は「政治的思想、宗教的若しくは哲学的信条を明らかにする個人データ」ではないため、それ自体はGDPR第9条に規定された機微な個人データではありません。
D) 不正解。GDPR第9条によると、労働組合員資格や、他の「（略）政治的思想、宗教的若しくは哲学的信条を明らかにする」個人データのみが機微な個人データです。

39 / 40
データ保護の役割のうち、個人データ取扱いの目的と手段を決定するのはどの役割ですか？

A) 管理者（コントローラ）
B) データ保護責任者(DPO)
C) 取扱者

A) 正解。管理者とは、単独で又は他と共同して、個人データの取扱いの目的及び手段を決定する自然人、法人、公的機関、行政機関又はその他の団体です。ソース：ホワイトペーパー -プライバシー、個人データ及びGDPR - §1.4役割、責任、ステークホルダ。
B) 不正解。
C) 不正解。

40 / 40
GDPRにおいて個人データと見なされる情報はどれですか？

A) たとえ真実でなくても、その人のプライバシーを害する可能性のある人物に関する情報
B) 識別可能な自然人に関するあらゆる情報
C) 識別可能な自然人に関するデジタル化された情報

A) 不正解。GDPRによると、識別可能な自然人に関するあらゆる情報は個人データです。
B) 正解。ソース：EU GDPR、ポケットガイド - 第2章 用語と定義 - 個人データ、GDPR第4条(1)。
C) 不正解。GDPRによると、識別可能な自然人に関するあらゆる情報は個人データです。

評価

次の表に、本模擬試験問題の正解を示します。

番号	正解	番号	正解
1	D	**21**	B
2	D	**22**	A
3	D	**23**	C
4	A	**24**	D
5	B	**25**	C
6	A	**26**	C
7	C	**27**	A
8	A	**28**	C
9	D	**29**	B
10	D	**30**	B
11	A	**31**	A
12	B	**32**	A
13	B	**33**	B
14	A	**34**	A
15	A	**35**	B
16	A	**36**	C
17	B	**37**	B
18	D	**38**	A
19	D	**39**	A
20	A	**40**	B

EXIN の連絡先

www.exin.com

YOUR ICT COMPETENCE PARTNER