模擬試験

2018 年 9 月版

目次

はじめに

これは EXIN Privacy and Data Protection Practitioner（PDPP.JP）です。この試験は EXIN 試験の規則および規定を適用します。

本試験は選択式の問題が 40 問で構成されます。各問題にはそれぞれ答の選択肢があり、その中の 1 つだけが正しい答となっています。

本試験では 1 問に正解する毎に 1 点が加算されます。最高得点は 40 点で、26 点以上が合格となります。

本試験の制限時間は 120 分です。

この試験において、GDPR を閲覧することが許可されています。文献 C-Eurlex - GDPR を閲覧するにはリンクをクリックして下さい。閉じる場合は、Navigator ボタンを使って Introduction（質問 1 の左にあるドット）をクリックし、リンクを再度クリックして下さい。

ご健闘を祈ります。

模擬試験

1 / 40
データの管理者（コントローラ）が、データ主体に対してアクセス可能にしなければならないのはどの文書ですか？

A) プライバシーポリシー
B) 利用規定
C) アクセス制御ポリシー
D) 情報セキュリティポリシー

2 / 40
ビジネスの観点で、適切なデータ保護とプライバシーポリシーの必須要件はどれですか？

A) 生産性と保護のバランスがとれていること
B) 契約と責任を定義していること
C) 違反について、どのように扱われるかを説明していること
D) ポリシーの必要性を説明していること

3 / 40
一般データ保護規則（GDPR）によれば、なぜ「プライバシーバイ・デフォルト」はプライバシー原則にとって不可欠なのですか？

A) 処理に関する特定の目的ごとに必要な個人データだけが処理されることを確実にするため
B) プライバシーポリシーに従い、デフォルトで個人データが収集されることを確実にするため
C) 個人データが処理される前に、デフォルトのプライバシーポリシーがデータ主体によって受け入れられることを確実にするため

4 / 40
ある企業は、消費者向けの新しい無料サービスを作るプロジェクトを構築しているところです。

プライバシーやデータ保護についての検討を開始するのに**最適な**タイミングはいつですか？

A) データ保護は、プロジェクトの実装段階で検討され実施される必要があります。
B) プライバシー及びデータ保護は、プロジェクトの開始時から推進される必要があります。
C) 個人データに関連するプロジェクトは、プロジェクト完了前に常にプライバシー監査を受ける必要があります。
D) このプロジェクトの目的は無料の消費者サービスを構築することであるため、データ保護は現行のプライバシー通知に基づく必要があります。

5 / 40
ある組織は、データ管理者（コントローラ）間のデータポータビリティを促進するような方法でデータ主体の個人データを保管するために、データ主体のためのサービスプロバイダとして、部門を新しく設置することを計画しています。その組織のCEOはあなたに助言を求めています。

データ保護管理システム(DPMS)を実装しなければならない理由はどれですか？

A) DPMSは重要なデータを一つのシステムに持込むのに役立つため
B) DPMSは、移転されるデータを収集するのに役立ち、セキュリティポリシーを作成する際に役立つため
C) DPMSはデータ管理を改善し、データ及び情報システムに対するリスクを軽減するため
D) DPMSは一般データ保護規則（GDPR）で必須とされているため

6 / 40
DPMSの構築準備段階で初期データの監査と評価をを実施しなければならない理由はどれですか？

A) データ監査と評価によって、個人のデータ保護及びプライバシーのリスクや課題、コンプライアンスリスクや組織のその他の関連するリスクが識別されるため
B) データ監査と評価によって、組織内外のデータフローの概要が明確になるため。これによってガバナンス監視委員会がデータフローを見直すことができます。
C) データ監査と評価によって、データ保護とプライバシーに関する役員会、経営陣、スタッフおよび従業員の準備状況や意識について分析することが可能となるため
D) データ監査と評価によって、全種類のデータがその組織のどこに配置され、それらのデータはその組織の誰によって所有されているかについての一覧（インベントリ）が提供されるため

7 / 40
あなたは、ABC社の新しい最高情報保護プライバシー責任者です。CEOは、社内及び外部関係者との間で収集、使用、開示される情報のプライバシーに関する適切な管理の欠如に懸念を抱いています。あなたは、データ保護管理システム(DPMS)の導入を準備する必要があるとCEOに勧めました。

このフェーズでは、データフローのインベントリ(一覧)が不可欠なのはなぜですか？

A) プライバシー問題に関する従業員の立場を確認するため
B) 軽減する必要があるデータ保護とプライバシーのリスクの明確な概要を把握するため
C) 従業員が個人的な事項と公的な会社の事項と混同している状況を特定するため
D) 従業員の仕事におけるプライバシー問題の意識を高めるため

8 / 40
段階2「データ保護とプライバシー組織」において、データ保護管理システム(DPMS)の導入に伴う組織的構造とメカニズムを確立するために必要なことは何ですか？

A) ギャップとエラーを特定するためのプライバシーとデータ保護のための対策と制御（コントロール）を監査すること
B) データ保護とプライバシーの意識を促すため、データ保護とプライバシーに関する考え方を全社で統合すること
C) DPMSの要件を満たすために、従業員はデータ保護およびプライバシープログラムの進捗についてを知る必要がある
D) データ保護プログラムのパフォーマンスを保証し、促進するために上級経営陣と定期的なコミュニケーションをとること

9 / 40
データ保護およびプライバシープログラムは、会社のプライバシーに関するミッションステートメントとして定着しています。

プライバシーに関するミッションステートメントにおいて重要**ではない**のはどの側面ですか？

A) 企業のミッションステートメントと適切かつ効果的に連携すること
B) データ保護とプライバシーの実務に関わる人の責任、職務、役割を設定すること
C) データ保護とプライバシーの戦略を詳細化すること
D) 会社がデータ保護とプライバシーに課す価値を強調すること

10 / 40
組織におけるデータ保護とプライバシープログラムの適切な実施を確実にするための重要な要素の一つに上級経営陣からの支援があります。

データ保護とプライバシープログラムにおいて上級経営陣からの支援を示すもの**ではない**のはどれですか？

A) データ保護とプライバシーの重要性をスタッフに伝達すること
B) データ保護とプライバシーに対する取組みの責任をデータ保護責任者(DPO)とプロセス所有者に委任すること
C) データ保護とプライバシーの活動を支援するための資金を提供すること

11 / 40
データ保護およびプライバシープログラムでは、個人データに必要な保護レベルを区別するために、データ分類システムを設計することが推奨されます。

データ分類システムの**主要な**目的はなんですか？

A) さまざまなカテゴリのデータに対して適切なラベリングをすること
B) さまざまなカテゴリのデータに対して適切なレベルのセキュリティとプライバシー制御（コントロール）を実装できるようにすること
C) 処理されたすべてのデータが確実に保護されるようにすること
D) さまざまなカテゴリのデータに対して対象グループごとにアクセスを制限すること

12 / 40
あなたは多国籍企業のデータ保護責任者（DPO）として雇われています。あなたの最初の仕事の1つは、企業のための一連のデータ保護とプライバシーの戦略、計画、方針を開発し、実装することです。

段階３の「データ保護とプライバシー：構築と実施」で**最初に**しなければならないことはなんです？

A) データ保護に関する会社のニーズと要件を分析し定義すること
B) 従業員の知識とデータ保護とプライバシーの概念を理解すること
C) 業界のベストプラクティスを調査し、自分の会社に適合させること
D) グローバルなデータ保護とプライバシーの状況を理解すること

13 / 40
一般データ保護規則（GDPR）の重要な要素の一つは、組織がコンプライアンスを実証する必要があるということです。

この観点から、データ保護管理システム（DPMS）のどの段階が**最も**重要ですか

A) 段階１。組織がプライバシーのために準備する
B) 段階２。プライバシーのための組織的な構造及びメカニズムを構築する
C) 段階３。組織のためのデータ保護とプライバシー対策が開発され実施される
D) 段階４。組織のプライバシーガバナンスのメカニズムが確立される

14 / 40
あなたは、データ保護責任者(DPO)として、データ保護とプライバシーのガバナンスに貢献するよう求められています。あなたは、個々のデータ主体に代わってプライバシー通知を行うことを決定しました。これらのプライバシー通知は、データの処理方法、制御（コントロール）についての情報をデータ主体に通知するものです。

プライバシー通知に含めるべき**ではない**のはどれですか？

A) 個人情報の収集、使用、維持、保管、開示の方法
B) 収集された個人データの内容
C) 組織が実施しているセキュリティポリシーの内容
D) データ主体が持つ詳細な制御（コントロール）

15 / 40
あなたはコンサルタント会社のデータ保護責任者（DPO）であり、インシデント管理システムを実装する必要があります。

インシデント管理システムで必要となるのはどれですか？

A) インシデント発生時にデータを抽出し、対応する手順（ステップ）を最小限に抑えるように、処理されたすべてのデータを記録し、安全な場所に保管すること
B) インシデントが発生したことを認識し、即時及び長期的な懸念事項に対応し、インシデントを追跡して、実施した手順（ステップ）が有効であることを確認すること
C) すべてのインシデントを登録し、プライバシー影響評価を実施してリスクを分析し、改善計画を立てること
D) すべてのインシデントを登録し、それらをガバナンス監視委員会に報告し、データフローを見直し、ガバナンス監視委員会が規定するセキュリティポリシーを改善すること

16 / 40
ある医療機関は、患者を監視するためのモバイルアプリケーションを開発するために2つの他の保健機関と緊密に連携しています。彼らは、新しいモバイルアプリケーションの結果を確認するためにパイロットを開始することに決めました。このパイロットでは、医療データに加えて、医師と患者の両方が、個人データと資格情報をモバイルアプリケーションに追加します。このパイロットのプロセスでは、セキュリティテストが実行されました。これらのテスト結果から、モバイルアプリケーションはまったく安全ではないことが判明しました。簡単にハッキングすることができ、患者のデータを変更できるような状況であり、医師の立場を乗っ取り、患者の医療情報を変更することも可能です。

3つの保健機関に指名されたデータ保護責任者(DPO)は、データ主体の利益を考慮して何をするべきでしょうか？

A) データ保護責任者(DPO)は、これがパイロットに過ぎず、患者全体のうち比較的小人数の患者が参加しているため、対応する必要はありません。
B) 検出された脆弱性の影響は、これがパイロットだけであるため、発生する可能性の高いリスクとは判断されないため、データ保護責任者(DPO)は措置を講じる必要はありません。
C) データ保護責任者(DPO)は、テスト結果は参加している患者及び医者に高いリスクをもたらす可能性が高いため、参加している患者及び医師に通知する必要があります。彼は監督当局にも通知する必要があります。
D) データ保護責任者(DPO)は、テスト報告書を使用して、セキュリティリスクをモバイルアプリケーションの必要な安全基準に合わせて調整し、監督当局にする必要があります。

17 / 40
外部機関にデータ保護とプライバシー評価の実施を委託する**主要な**理由は何ですか？

A) 自社のプライバシー活動と業界標準とを比較するベンチマークテストをするため
B) 社内のプライバシーポリシーと適用される法的要件への遵守を独立した立場で検証するため
C) 自社のデータ保護およびプライバシープログラムの信頼性を向上させるため
D) 自社のデータ保護とプライバシープログラムにおいて時間と予算の制約が主要な検討事項であるため

18 / 40
ある会社は、顧客関係管理（CRM）システムの停止を2時間以上引き起こした個人データの侵害に直面しています。この会社のデータ保護責任者（DPO）として、あなたは、とりわけアドホック的な（暫定的な）プライバシー評価を行うことを決めました。

このアドホック的な評価の**主要な**目的の一つは何ですか？

A) 顧客への適切なメッセージを助言するため
B) この侵害による被害の程度を評価するため
C) プライバシーリスクを判断するため
D) この侵害の責任者を特定するため

19 / 40
データ管理者（コントローラ）である企業は、財政難に直面しており、取締役会はデータ保護管理システム（DPMS）のソフトウェアを更新しないことに決めました。代わりに、彼らはデータ保護認証を適用するために、監督当局に承認を要求しました。これにより、会社は多くの資金を節約し、より商業的価値を高めることができます。

もしあなたがこの管理者（コントローラ）のデータ保護責任者(DPO)なら、取締役会にどのような助言をしますか？

A) データ保護認証を取得するためのプロセスを継続する。取得した認証は管理者（コントローラ）としての義務を順守していることを実証するのに使用することができます。
B) 外部のデータ保護とプライバシーの評価を実行する。これは予算を全部使うことになるが、その性質、範囲、文脈の中で適切な技術的および組織的措置が取られることを確実にします。
C) 社内評価でもっとも脆弱性が高く、更新が必要だと判明した部分だけを更新して、本来更新するべきDPMSの3分の1だけの更新を実施します。
D) DPMSへの更新を実施する。 DPMSの更新に失敗すると、管理者（コントローラ）として適切な技術的および組織的措置を講じていないとみなされる可能性があるため、遵守違反となる潜在的なリスクが発生します。

20 / 40
あるパリ中心部の人気フィットネスクラブは、同じくパリにあるホスティング会社にデータを保管しています。フィットネスクラブの会員のデータが保管されているサーバは最近ITサービス会社による定期点検を受けました。ITサービス会社が訪れた翌日、サーバが故障し、サーバルーム内で火事が発生しました。この火事によってフィットネスクラブのデータは喪失し、同じサーバ上に保管されていたバックアップも失われました。調査によってサーバルームの冷却システムに不具合があり、サーバシステムのオーバーヒートが発生したことが判明しました。保守エンジニアは、その室内の温度が少々高いことに気づいていましたが、急いでいたため及び、それほど異常だとは感じなかったため、このことをサーバ会社には報告しませんでした。冷却システムはホスティング会社自身のサービスに含まれます。

このインシデントに対して責任がある可能性が**最も**高いのはどの関係者ですか？

A) フィットネスクラブ。喪失したデータの所有者である組織のため
B) フィットネスクラブ。バックアップを他のサーバに保管するよう依頼しなかったため
C) ホスティング会社。個人データ周辺のセキュリティに責任があるため
D) IT会社。保守エンジニアはサーバルームの温度がかなり高いことを報告する義務があったため

21 / 40
ある病院は患者の請求書の印刷を印刷会社に委託しました。印刷会社は、他の組織の請求書も印刷しています。名前と住所が印刷会社で仕分けられた際に混同されたため、間違った患者に複数の請求書が送付されました。病院は慎重に事業を分析していました。同病院は、堅牢な検証プロセスが実装されており、印刷会社とも契約上の契約を結んでいました。

印刷会社が責任を負う可能性が高いのはなぜですか？

A) 印刷会社が取扱い活動の目的を決定するため
B) 印刷会社が印刷手続を決定するため
C) 印刷会社が、どのデータを処理するかを決定するため
D) 印刷会社が他の組織の請求書を印刷しているため

22 / 40
ある家族経営の住宅設備の小売店は、対象を絞った広告とマーケティングのためにウェブサイト分析会社と連動することを決定しました。地元の医師と弁護士は、他のクライアントもいる同じウェブサイト分析会社と連動することを決めました。

データ保護責任者(DPO)を指名する必要があるのはどの組織ですか？

A) 家族経営の住宅設備の小売店
B) 家族経営の住宅設備の小売店とウェブサイト分析会社
C) 医師と弁護士
D) ウェブサイト分析会社

23 / 40
オランダに面する北海に浮かぶ小さな島、テッセル島に一次医療の医師がいます。彼はプライベート（利益）組織を所有しています。彼の医療行為は登録された60人に及びます。

データ保護責任者(DPO)を指名する必要があるかどうかに関して正しく記述しているのはどれですか？

A) この医療行為は、大規模な医療データと管理と取扱いを行う業務とみなすには規模が小さすぎるため、この一次医療の医師はデータ保護責任者(DPO)を指名する必要はありません。
B) 医療行為は定期的かつ体系的に患者を健診するため、医師はDPOを任命する義務があります。
C) この一次医療の医師は、この島で唯一の医療行為を行っています。彼は彼の患者に関して独立した専門的な役割を果たしています。彼は同時に医師とデータ保護責任者(DPO)の役割を兼ねることができます。

24 / 40
一般データ保護規制（GDPR）の下では、データ保護責任者（DPO）は、業務の実行に関する秘密または機密性に拘束されます。

データ保護責任者(DPO)がこの秘密や機密性の制約を受けずに助言を求めることができるのはどの当事者との関係においてですか？

A) 自社の取締役会
B) データ保護とプライバシーネットワークメンバのチーム
C) 情報セキュリティ責任者(ISO)
D) 監督機関

25 / 40
あなたはある高級ファッションの百貨店チェーンでデータ保護責任者(DPO)として雇用されています。同社は、正規の顧客を識別してより良いサービスを提供するために、顔認識ソフトウェアを購入する意向を表明しています。アカウントを保持しているすべての顧客にこの変更が通知され、オプトアウトの選択肢が提供される予定です。

データ保護影響評価(DPIA)を事前に実施することをあなたが推奨すべき理由はどれですか？

A) ISO27001によると、DPIAは情報セキュリティマネジメントシステム(ISMS)の必須項目であるため
B) DPIAを実施し、経営陣による承認を得て、将来のセキュリティインシデントに対する責任を負う可能性をなくすことはグッドプラクティス（良い慣行）の一環であるため
C) GDPRでは、プロファイリングや大量のモニタリングを通じて、個人情報の保護に影響を与える可能性のある新しい技術が使用される場合、DPIAが必須であると規定しているため
D) GDPRでは、現行のプロセス、プロジェクト、またはポリシーの変更に対してDPIAは必須であると規定しているため

26 / 40
あなたは、大規模な組織で働いているとします。あなたの所属する組織は、コンピュータ上の作業に関する従業員の監視を容易にするソフトウェアツールを使用しています。これらのツールは、一般的なアルゴリズムと時間を示す指標に基づいて、休憩やストレッチが必要なタイミングを示します。休憩時間についての助言をより適切にパーソナライズするために、監視ツールを心拍計に接続することで機能性を追加することが発案されました。

DPIAを実施しなければならない理由はどれですか？

A) 新しいツールやプロセスにはDPIAが必須であるため
B) このツールは従業員を監視することにより個人データの取扱いを含むようになるため
C) これは機微な個人データの処理を含む新しいアプリケーションであるため
D) これは公的な場における大規模な行動観察を含む新しいアプリケーションであるため

27 / 40
あなたは、運輸省（Ministry of Transportation）最高プライバシー責任者として新しい仕事を始めました。新しく国道の人々の運転行動を監視するためのプロジェクトが発表されました。同部では知的なビデオ分析システムを使用して車を選別し、ナンバープレートを自動的に認識することを想定しています。ある朝、国務長官があなたのオフィスを訪れました。長官は明らかにプロジェクトの開始を急いでいるようで、プライバシー問題によって望ましくない遅れが引き起こされるかもしれないという懸念を明らかにしました。

あなたは長官に何を言うべきですか？

A) これは、自分の権限をはるかに上回る国家的にも重要な課題であることから、監督機関に連絡をとることを長官に依頼する
B) 想定されているデータ取扱いの性質はDPIAによる精査を要求するものであることを長官に伝える。生じるリスクと緩和対策をプロジェクト計画に組み込む必要がある
C) 国民に処理活動の目的と範囲について適切に通知している限り、DPIAの必要がないことを長官に通知します。
D) GDPRでは大規模な監視やプロファイリングなどの「高リスク」なデータ処理業務が禁止されているため、プロジェクトは真剣に再考をするべきだと長官に伝える

28 / 40
GDPRは特定の条件下でデータ保護影響評価(DPIA)を実施する必要があることを規定していますが、実際*どのように*実施するかについては記述していません。それでも、GDPRはDPIAから得られる望ましい成果の最小限のセットを明確に特定しています。

この最小限の望ましい成果を考慮した場合、**常に**DPIAに含まれるべき活動はどれですか？

A) データ主体の権利を保護するため、主体によるアクセス要求手続を開発する
B) 処理される個人データと処理の目的を識別する
C) データ主体に分析が実施されることを通知し、明確な同意を要求する
D) インシデント対応計画を作成し、データ侵害を回避する適切な保護措置を定義する

29 / 40
ある会社は、トレンドを検知・分析し、予測を改善できるように顧客データをより有効に活用することを決定しました。新たな組織的ユニットが設立される予定です。データの専門家は最新のデータ分析ツールを使ってデータウェアハウスを構築する予定です。

データ保護責任者(DPO)の役割を持つあなたは、このことがデータ主体の権利に悪影響を及ぼす高リスクな試みであると深い懸念を示しました。しかし、CIOとCEOの両方が開発を進めることを望んでおり、あなたの懸念に対応することには消極的です。

とるべき行動として**最適**なのはどれですか？

A) DPIAを実施し、取締役会及びその他の利害関係者とDPIAの結果及び可能な緩和策について議論する
B) CIOにデータの匿名化を関与させることによりGDPRが適用されないようにする
C) 顧客に相談し、現行の処理について明示的な同意を求める顧客アンケートを設定する
D) 監督機関に連絡し、意図している処理について見解を求め、リスク説明についての助言を依頼する

30 / 40
なぜデータ保護影響評価（DPA）は組織のリスク管理の一環とみなされるのでしょうか？

A) DPIAは、その組織が軽減しなければならないデータ主体のリスクを識別するものであるため
B) DPIAは、その組織が軽減しなければならない組織のセキュリティリスクを識別するものであるため
C) DPIAは、リスクを分類するために必要な影響を測定するものであるため
D) DPIAは、組織がGDPRを順守するのに必要であるため

31 / 40
データ保護影響評価(DPIA)では、プライバシーに対するリスクを特定することが重要です。次の段階では、これらのリスクを排除するか、受容レベルまで軽減することです（リスク対応）。

典型的なリスク対応を構成するのはどの行動ですか？

A) 有効性の指標を定義する
B) 収集したデータの量を削減する
C) プライバシーリスクの登録を設定する
D) DPIAの結果を承認し、記録する

32 / 40
データ保護インパクトアセスメント（DPA）を実施する必要がある場合、GDPRにはいくつかの要素が必要となります。これらの要素のうちの2つは、比例原則と必要性の評価及び特定されたリスクを緩和するための対策の評価です。

GDPRの規定によってDPIAに含める必要がある他の要素はどれですか？

A) データ侵害の対処方法に関する手順
B) DPIAの結果に関する公式報告書（公表）
C) データ主体に及ぼすプライバシーに関するリスクの評価

33 / 40
あなたは、個人データの処理を含む組織内のプロジェクトに対して責任を負います。責任の一部として、データ保護影響評価（DPA）を実行し、データマッピングを開始することを決定しました。

DPIAプロセスにおいてデータマッピングが役立つ理由はどれですか？

A) 個人データに対するリスクの概要を得るのに役立つため
B) データ処理に用いられるシステムの概要を得るのに役立つため
C) 処理の目的を識別するのに役立つため

34 / 40
ある組織は、プロファイリングに基づいて顧客に対して自動化された意思決定を行う予定です。

データ保護影響評価(DPIA)のプロセスのうち、特に注意を払うのに**最も適した**側面はどれですか？

A) この処理活動に関連してDPIAを実行する必要性の評価
B) データがいつ消去されるかの評価
C) 人の介入を促進することによってデータ主体の権利を保護するための対策
D) データを保護し、データ主体がデータにアクセスできないようにするための対策

35 / 40
あなたは、組織内でデータ保護影響評価(DPIA)の責任を負っています。このDPIAに伴って、想定される処理活動と目的について適切な記述を作成するために、あなたは多くの同僚と話し合いました。この協議の間、処理には現在の目的には厳密には必要ではないが、将来の目的のために使用できる個人データの収集を含むことが判りました。収集を現在のプロセスに合わせる方が効率が上がります。

あなたはこの状況で何をすべきですか？

A) GDPRの第6条に示すように、効率性は組織の正当な利益であるため、その処理を許可します。
B) DPIAが実行される処理の目的に必要でないため、追加データを収集しないことを要求します。
C) その追加データの処理に関してGDPRの第6条に則った正当な事由を示すよう同僚に要求し、取扱いを許可します。
D) データ侵害を防止するため、そのデータが適切に保護されることを要求します。

36 / 40
あなたは会社が提供する新しいサービスのためにDPIAを実行しています。このサービスでは必然的に顧客の個人データの大規模処理を必要とします。処理には正当な理由と目的があり、関連するデータ主体の権利に対するリスクを軽減するための適切な措置が実施される予定です。しかし、サービスが成功するためには、顧客による受け入れが重要であることは明らかです。

この場合、データ保護影響評価(DPIA)プロセスを完了するのに必要となる具体的な行動はどれですか？

A) 顧客またはその代理人に相談して、個人データの処理に関する意見を求める。
B) 処理の適法性について確認をとるためにデータ保護機関(DPA)に相談する
C) ヘルプデスクを開設し、サービスを公表後、顧客がそのサービスについて説明を受けられるようにする。
D) 顧客にDPIA報告書（データ保護影響評価報告書）を送り、対策がとられることを保証する

37 / 40
あなたは、国際的な顧客を持つ大規模な物流会社のデータ保護責任者（DPO）としての責任を負います。35人の従業員の人事情報を含む暗号化されたメモリースティックを紛失したか、置き忘れたと人事部門長が報告してきました。

一般データ保護規則（GDPR）において、これをデータ侵害として監督機関に報告する必要があるのはなぜですか？

A) 機密性の高い会社データの損失を伴うセキュリティインシデントは、データ侵害として報告する必要があります。
B) 個人データが含まれたデバイスの紛失は自然人の権利及び自由に対するリスクであるため、このインシデントは報告する必要があります。
C) 監督機関が35人の従業員に侵害があったことを通知できるよう、このインシデントは不当な遅滞なしに報告される必要があります。

38 / 40
組織がデータ侵害を監督当局に報告する必要があるのは、どのような場合ですか？

A) インシデントが自然人の権利と自由に対するリスクをもたらす可能性がある場合すべて
B) 自然人の権利と自由を危険にさらすキュリティ上の脅威がある場合すべて
C) インシデント発生後72時間以内に組織がそのインシデントを解決できない場合のみ
D) インシデント発生後72時間以内にインシデントが認識された場合のみ

39 / 40
組織が関係するデータ主体にデータ侵害を報告する必要があるのはどのような状況ですか？

A) データ侵害が自然人の権利と自由に対する「高いリスク」をもたらす可能性がある場合すべて
B) 関係するデータ主体の権利と自由を危険にさらすセキュリティインシデントが発生した場合すべて
C) データ主体にデータ侵害を通知する必要があると監督機関が判断した場合のみ
D) サイバー犯罪者などの外部の犯行者によって個人データが危険にさらされる「悪意」が存在する場合のみ

40 / 40
すべての組織は、監督当局に通知されなければならないデータ違反を処理する必要があります。通知プロセスは繰り返されるため、以下のような要素を含む報告書のテンプレートを設定することが推奨されます。

・個人データ侵害の性質
・侵害によって起こりうる影響
・緩和するための対策

このテンプレートに追加すべき項目はどれですか？

A) ・CEO の名前と連絡先の詳細
・インシデント対応計画
B) ・影響を受けるデータ被験者の名前
・侵害の責任者の名前
C) ・影響を受けるデータ主体の人数
・データ保護責任者(DPO)の名前と連絡先の詳細
D) ・セキュリティインシデントの件数
・サイバーセキュリティの脅威分析

解答集

1 / 40
データの管理者（コントローラ）が、データ主体に対してアクセス可能にしなければならないのはどの文書ですか？

A) プライバシーポリシー
B) 利用規定
C) アクセス制御ポリシー
D) 情報セキュリティポリシー

A) 正解。GDPRでは、プライバシーポリシーをデータ主体に対してアクセス可能にすることが必要です。文献A、第16章の段落Using policies to demonstrate compliance参照。(E-book page 155/164: “Your privacy policy should be readily accessible...”)
B) 不正解。この文書にデータ主体がアクセスできるようにする必要はありません。
C) 不正解。この文書にデータ主体がアクセスできるようにする必要はありません。
D) 不正解。この文書にデータ主体がアクセスできるようにする必要はありません。

2 / 40
ビジネスの観点で、適切なデータ保護とプライバシーポリシーの必須要件はどれですか？

A) 生産性と保護のバランスがとれていること
B) 契約と責任を定義していること
C) 違反について、どのように扱われるかを説明していること
D) ポリシーの必要性を説明していること

A) 正解。文献A、第16章の段落Using policies to demonstrate compliance参照。(e-book page 156/164)
B) 不正解。これは適切なポリシーの必須要件ではありません。
C) 不正解。これは適切なポリシーの必須要件ではありません。
D) 不正解。これは適切なポリシーの必須要件ではありません。

3 / 40
一般データ保護規則（GDPR）によれば、なぜ「プライバシーバイ・デフォルト」はプライバシー原則にとって不可欠なのですか？

A) 処理に関する特定の目的ごとに必要な個人データだけが処理されることを確実にするため
B) プライバシーポリシーに従い、デフォルトで個人データが収集されることを確実にするため
C) 個人データが処理される前に、デフォルトのプライバシーポリシーがデータ主体によって受け入れられることを確実にするため

A) 正解。文献A第5章の段落Privacy by design and default参照。（e-book: 67/164）: “The controller shall implement appropriate….”
B) 不正解。プライバシーバイ・デフォルトはデータ収集とは関連しません。
C) 不正解。プライバシーバイ・デフォルトは同意とは関連しません。

4 / 40
ある企業は、消費者向けの新しい無料サービスを作るプロジェクトを構築しているところです。

プライバシーやデータ保護についての検討を開始するのに**最適な**タイミングはいつですか？

A) データ保護は、プロジェクトの実装段階で検討され実施される必要があります。
B) プライバシー及びデータ保護は、プロジェクトの開始時から推進される必要があります。
C) 個人データに関連するプロジェクトは、プロジェクト完了前に常にプライバシー監査を受ける必要があります。
D) このプロジェクトの目的は無料の消費者サービスを構築することであるため、データ保護は現行のプライバシー通知に基づく必要があります。

A) 不正解。実装段階では遅すぎます。プライバシーとデータ保護は、プライバシーバイ・デザインの概念に従ってプロジェクトの開始時点から推進する必要があります。
B) 正解。文献A、第5 章の段落Privacy by design and default参照。これがプライバシーバイ・デザインの概念です。
C) 不正解。プロジェクト完了時点では遅すぎます。プライバシーとデータ保護は、プライバシーバイデザインの概念に従ってプロジェクトの開始時点から推進する必要があります。
D) 不正解。プロジェクトの成果に関わらず、プライバシーとデータ保護は、プライバシーバイ・デザインの概念に従ってプロジェクトの開始時点から推進されなければなりません。

5 / 40
ある組織は、データ管理者（コントローラ）間のデータポータビリティを促進するような方法でデータ主体の個人データを保管するために、データ主体のためのサービスプロバイダとして、部門を新しく設置することを計画しています。その組織のCEOはあなたに助言を求めています。

データ保護管理システム(DPMS)を実装しなければならない理由はどれですか？

A) DPMSは重要なデータを一つのシステムに持込むのに役立つため
B) DPMSは、移転されるデータを収集するのに役立ち、セキュリティポリシーを作成する際に役立つため
C) DPMSはデータ管理を改善し、データ及び情報システムに対するリスクを軽減するため
D) DPMSは一般データ保護規則（GDPR）で必須とされているため

A) 不正解。DPMSは、システムにデータを収集するのではなく、組織のデータ管理を改善し、企業のデータが直面するリスクを軽減することを目的としています。
B) 不正解。DPMSはデータを収集することが目的ではなく、セキュリティポリシーの作成と実装はDPMSの一部にすぎません。DPMSには方法論、戦略、一連のポリシーや手続、技術的なツールや他のツールも含まれます。
C) 正解。DPMSはデータ管理を改善すると同時に次のようなリスクの軽減を重視するシステムです。
・ データのハッキング、盗難、喪失される可能性があること
・ 従業員のデータに関するセキュリティ意識が不十分であること。
・ 組織が、方法論、戦略及び一連のポリシー、手続、技術的及びその他のツールを開発することにより、プライバシー規定を順守しなくなった場合、大変高額な罰金が課せられる（文献B、段落2.1 Introduction to phase 1）
D) GDPRは、組織的および技術的措置によってデータを適切に保護する必要がありますが、対策の形式は規定されていません。従って、DPMSについても規定されていません。

6 / 40
DPMSの構築準備段階で初期データの監査と評価をを実施しなければならない理由はどれですか？

A) データ監査と評価によって、個人のデータ保護及びプライバシーのリスクや課題、コンプライアンスリスクや組織のその他の関連するリスクが識別されるため
B) データ監査と評価によって、組織内外のデータフローの概要が明確になるため。これによってガバナンス監視委員会がデータフローを見直すことができます。
C) データ監査と評価によって、データ保護とプライバシーに関する役員会、経営陣、スタッフおよび従業員の準備状況や意識について分析することが可能となるため
D) データ監査と評価によって、全種類のデータがその組織のどこに配置され、それらのデータはその組織の誰によって所有されているかについての一覧（インベントリ）が提供されるため

A) 正解。この段階でのデータ監査と評価によって、コンプライアンスや個人に関わるリスクや他の関連するリスクが識別されます。この結果からDPMSに含めるべき対象についての最初の洞察が得られます。（文献B、段落2.2.1. Phase 1: Data Protection and Privacy Preparation, AP#4 Perform Initial Data Audits and Assessments. ）
B) 不正解。データの監査と評価は、組織内外のデータフローのフローチャートの文書化や維持するシステムの開発と実装には使用されません。。また、ガバナンス監視委員会がデータフローを見直すことはありません。ガバナンス監視委員会は潜在的なプライバシーとデータ保護の影響及びリスクを見直し、それらのリスクを軽減するための対策及び制御を確実にします。
C) 不正解。役員会、経営陣、スタッフおよび従業員のデータ保護とプライバシーに関して準備状況や意識を分析するのにデータ監査と評価はあまり用いられません。データ監査と評価は、より広範な観点からリスクに関する洞察を提供するものです。
D) 不正解。全種類のデータがその組織のどこに配置され、それらのデータはその組織の誰によって所有されているかについての一覧（インベントリ）を作成するのにデータ監査と評価は使いません。データ監査と評価はリスクを識別するために使います。

7 / 40
あなたは、ABC社の新しい最高情報保護プライバシー責任者です。CEOは、社内及び外部関係者との間で収集、使用、開示される情報のプライバシーに関する適切な管理の欠如に懸念を抱いています。あなたは、データ保護管理システム(DPMS)の導入を準備する必要があるとCEOに勧めました。

このフェーズでは、データフローのインベントリ(一覧)が不可欠なのはなぜですか？

A) プライバシー問題に関する従業員の立場を確認するため
B) 軽減する必要があるデータ保護とプライバシーのリスクの明確な概要を把握するため
C) 従業員が個人的な事項と公的な会社の事項と混同している状況を特定するため
D) 従業員の仕事におけるプライバシー問題の意識を高めるため

A) 不正解。データ保護やプライバシーの文脈では、プライバシー分析でプライバシー問題に関して個々の従業員の見解や意見を求めることはありません。
B) 正解。この分析では、企業が所有するデータは何か、アクセス、共有、使用に関するリスクがどこにあるか、を明らかにします。これにより会社は、事業に与える影響を最小限に抑えながら、これらのリスクを緩和するための行動計画を立案することが可能となります。文献B、DPMS, Phase 1- Preparations, Products and outcome参照。
C) 不正解。プライバシー分析は、個々の従業員の私的事項には関係しません。
D) 不正解。従業員が情報収集に関与する場合、副次的効果があるかもしれませんが、本来の目的ではありません。従業員の意識向上は、プライバシー研修を実施する段階3に含まれます。

8 / 40
段階2「データ保護とプライバシー組織」において、データ保護管理システム(DPMS)の導入に伴う組織的構造とメカニズムを確立するために必要なことは何ですか？

A) ギャップとエラーを特定するためのプライバシーとデータ保護のための対策と制御（コントロール）を監査すること
B) データ保護とプライバシーの意識を促すため、データ保護とプライバシーに関する考え方を全社で統合すること
C) DPMSの要件を満たすために、従業員はデータ保護およびプライバシープログラムの進捗についてを知る必要がある
D) データ保護プログラムのパフォーマンスを保証し、促進するために上級経営陣と定期的なコミュニケーションをとること

A) 不正解。全面的な実装が完了した後に初めて監査を実施することができます。これは段階5についての結果です。
B) 正解。企業が満たさなければならない要件を順守するためにとるべき段階や行動について、データ保護とプライバシーに関する認識が不可欠です。データ保護とプライバシーを改善するには、その組織のすべての従業員、スタッフ、上級経営陣の間で十分に高められたデータ保護とプライバシーに関する認識に基づいて、継続的な処理を監視することが必要です。
（文献B、段落2.2.2., Step OS# 5, see 5.2 section e）
C) 不正解。従業員がプログラムの状況について知ることは重要ですが、これによって組織的な構造やメカニズムが構築されるということではありません。
D) 不正解。定期的なコミュニケーションは一般的に組織構造と仕組みの確立に直接つながるものではなく、また、コミュニケーションをする相手を上級経営陣に限定すべきではありません。

9 / 40
データ保護およびプライバシープログラムは、会社のプライバシーに関するミッションステートメントとして定着しています。

プライバシーに関するミッションステートメントにおいて重要**ではない**のはどの側面ですか？

A) 企業のミッションステートメントと適切かつ効果的に連携すること
B) データ保護とプライバシーの実務に関わる人の責任、職務、役割を設定すること
C) データ保護とプライバシーの戦略を詳細化すること
D) 会社がデータ保護とプライバシーに課す価値を強調すること

A) 不正解。データの保護とプライバシーを会社の機能、活動、プロセスに組み込む必要があるため、プライバシーに関するミッションステートメントを企業の宣言文に合わせることは重要な原則です。
B) 正解。実践について詳しく設定することは、データ保護とプライバシーの導入の際に取組むものであるため、プライバシーに関するミッションステートメントにいては重要な原則ではありません。（文献B、段落2.2.2, Step OS#1, see 1.5 in conjunction with step OS#2）
C) 不正解。データ保護とプライバシーの戦略を詳述することは、その会社でデータ保護とプライバシーをどのように実施するかについて全体的な方向を規定するため、重要な原則の一つです。
D) 不正解。会社がデータ保護とプライバシーに置いている価値を強調することは、データ保護とプライバシーに対するその会社のコミットメントを表すため、重要な原則です。

10 / 40
組織におけるデータ保護とプライバシープログラムの適切な実施を確実にするための重要な要素の一つに上級経営陣からの支援があります。

データ保護とプライバシープログラムにおいて上級経営陣からの支援を示すもの**ではない**のはどれですか？

A) データ保護とプライバシーの重要性をスタッフに伝達すること
B) データ保護とプライバシーに対する取組みの責任をデータ保護責任者(DPO)とプロセス所有者に委任すること
C) データ保護とプライバシーの活動を支援するための資金を提供すること

A) 不正解。すべての管理者やスタッフにデータ保護とプライバシーの重要性を伝えることは、上級経営陣のコミットメントと支援を示しています。
B) 正解。データ保護責任者(DPO)にデータ保護とプライバシーに関するすべての責任を委任することは、上級経営陣の支援を示すものではありません。上級経営陣は任務を委任できますが、責任は委任できません。（文献B、段落2.2.2, Step OS#3, see 2.2）
C) 不正解。データ保護とプライバシー活動を支援するのに十分な資金を確保することは、上級経営陣が必要な箇所に資金を割り当てていることを示します。

11 / 40
データ保護およびプライバシープログラムでは、個人データに必要な保護レベルを区別するために、データ分類システムを設計することが推奨されます。

データ分類システムの**主要な**目的はなんですか？

A) さまざまなカテゴリのデータに対して適切なラベリングをすること
B) さまざまなカテゴリのデータに対して適切なレベルのセキュリティとプライバシー制御（コントロール）を実装できるようにすること
C) 処理されたすべてのデータが確実に保護されるようにすること
D) さまざまなカテゴリのデータに対して対象グループごとにアクセスを制限すること

A) 不正解。ラベリングは、データ分類の異なるレベルを示すために必要ですが、主要な目的ではなく実装するための活動です。
B) 正解。データ分類システムの主な目的は、データの機密性と機密性のさまざまなレベルに対して適切なレベルのセキュリティとプライバシー制御を実装できるようにすることであり、これが最適な解答です。（文献B、段落2.2.3, Step DI#1, see 2.1-2.2）
C) 不正解。これはあまりにも幅広く一般的な目的であり、異なるレベルのセキュリティと保護を区別していません。
D) 不正解。データ分類システムを使用して、異なるデータカテゴリに対してアクセスを制限することは、ユーザの対象グループごとではなく、ユーザが保持する職務と「知る必要性（need to know）」ごとです。

12 / 40
あなたは多国籍企業のデータ保護責任者（DPO）として雇われています。あなたの最初の仕事の1つは、企業のための一連のデータ保護とプライバシーの戦略、計画、方針を開発し、実装することです。

段階３の「データ保護とプライバシー：構築と実施」で**最初に**しなければならないことはなんです？

A) データ保護に関する会社のニーズと要件を分析し定義すること
B) 従業員の知識とデータ保護とプライバシーの概念を理解すること
C) 業界のベストプラクティスを調査し、自分の会社に適合させること
D) グローバルなデータ保護とプライバシーの状況を理解すること

A) 正解。まず、企業のニーズと要件を理解し、定義し、データ保護とプライバシーに関する戦略、計画、ポリシーの目的と目標を確立することです（文献B、段落2.2.3, Step DI#1）
B) 不正解。法人のニーズと要件を分析し定義した後にのみこれを行うことができます。
C) 不正解。業界のベストプラクティスを自分の会社に適合させることができるのは、会社のニーズと要件の分析と定義が完了してからです。
D) 不正解。何が関連するかを判断できるのは、会社のニーズと要件の分析と定義が完了してからです。

13 / 40
一般データ保護規則（GDPR）の重要な要素の一つは、組織がコンプライアンスを実証する必要があるということです。

この観点から、データ保護管理システム（DPMS）のどの段階が**最も**重要ですか?

A) 段階１。組織がプライバシーのために準備する
B) 段階２。プライバシーのための組織的な構造及びメカニズムを構築する
C) 段階３。組織のためのデータ保護とプライバシー対策が開発され実施される
D) 段階４。組織のプライバシーガバナンスのメカニズムが確立される

A) 不正解。段階１では実装の準備をしますが、まだコンプライアンスの形式は含まれていません。この段階での具体的な目的は、データ保護及びプライバシーの要件と企業に影響を与えるニーズを分析すること、データ保護およびプライバシーに関連する法令、標準及び規制を収集すること、必要なリソースを備えた行動計画を立てることです。このことにより、会社は現存のデータ保護とプライバシーの規定や規則を十分考慮した上で個人データ、活動、取引、処理について管理をする準備ができます。
B) 不正解。段階２では、プライバシー要件を実装するための基礎を設定するために重要ですが、コンプライアンスは含まれていません。この段階での具体的な目的は、データ保護とプライバシープログラムを設計し、データ保護およびプライバシー責任者を設定することです。データ保護とプライバシーに関わるすべての関係者に従事しコミットすることです。
C) 正解。手続、ポリシー、制御（コントロール）の実装はコンプライアンスを示します。この段階３での具体的な目的は、データ分類システムを設計すること、企業や組織のデータ保護とプライバシーに関する法律や要件を実施するために必要なすべてのポリシー、手続、制御（機微データの管理、教育計画の実行、プライバシーを業務に組込むなど）を構築し実施することです。（文献B、段落2.2.3, introduction Goal and objectives, and step #DI 5 Execute DPP Integration Activities, and Phase 3 Implementation and outcomes, and Literature C GDPR Article 24(1).）
D) 不正解。段階４はコンプライアンスを維持する上で重要ですが、最初に実装が必要です。この段階での具体的な目的は、データ保護とプライバシーのガバナンス構造（データ保護とプライバシープログラム、データ保護とプライバシー責任者、多くの場合データ保護とプライバシー委員会など）を設計及び設定し、データ保護とプライバシーに関わるすべての関係者に従事しコミットすること、会社または組織のデータ保護とプライバシーの問題をすべて継続的に報告することです。

14 / 40
あなたは、データ保護責任者(DPO)として、データ保護とプライバシーのガバナンスに貢献するよう求められています。あなたは、個々のデータ主体に代わってプライバシー通知を行うことを決定しました。これらのプライバシー通知は、データの処理方法、制御（コントロール）についての情報をデータ主体に通知するものです。

プライバシー通知に含めるべき**ではない**のはどれですか？

A) 個人情報の収集、使用、維持、保管、開示の方法
B) 収集された個人データの内容
C) 組織が実施しているセキュリティポリシーの内容
D) データ主体が持つ詳細な制御（コントロール）

A) 不正解。これは2.2.4項のステップGR #2で規定された、個人に対して実施すべきプライバシー通知に含まれます。
B) 不正解。これは2.2.4項のステップGR #2で規定された、個人に対して実施すべきプライバシー通知に含まれます。
C) 正解。プライバシー通知は組織が実装しているセキュリティポリシーを特定するものではありません。組織が個人向けのセキュリティポリシーを明らかにした場合、ハッキングのリスクが増大し、個人データを守るという個人の利益に反することになります。プライバシー通知は、個人が個人情報を入手する権利、データの収集と処理について学び、データを管理する権利に関してのみ行う必要があります。（文献B、段落2.2.4., step GR # 2, see 2.2.4）
D) 不正解。これは2.2.4項のステップGR #2で規定された、個人に対して実施すべきプライバシー通知に含まれます。

15 / 40
あなたはコンサルタント会社のデータ保護責任者（DPO）であり、インシデント管理システムを実装する必要があります。

インシデント管理システムで必要となるのはどれですか？

A) インシデント発生時にデータを抽出し、対応する手順（ステップ）を最小限に抑えるように、処理されたすべてのデータを記録し、安全な場所に保管すること
B) インシデントが発生したことを認識し、即時及び長期的な懸念事項に対応し、インシデントを追跡して、実施した手順（ステップ）が有効であることを確認すること
C) すべてのインシデントを登録し、プライバシー影響評価を実施してリスクを分析し、改善計画を立てること
D) すべてのインシデントを登録し、それらをガバナンス監視委員会に報告し、データフローを見直し、ガバナンス監視委員会が規定するセキュリティポリシーを改善すること

A) 不正解。データの記録化と保持はデータストレージの一部にすぎません。バックアップを作成することは、インシデント自体を管理するのではないため、インシデント処理のプロセスを改善するものではありません。
B) 正解。これはインシデント管理サイクルです。（文献A、第14章 p. 241（e-book 135））
C) 不正解。インシデント管理システム自体は、プライバシーの影響評価を含んでいません。プライバシー影響評価は、例えば（部分的に）新しいシステム、アプリケーション、またはソフトウェアを使用してデータを処理する場合にのみ重要となります。
D) 不正解。インシデントは責任ある担当者に報告されなければなりません。ガバナンス監視委員会は、これらのデータフローを見直すことはありません。委員会は潜在的なプライバシーとデータ保護の影響とリスクを見直し、これらのリスクを軽減するための適切な対策と制御（コントロール）を確実にします。

16 / 40
ある医療機関は、患者を監視するためのモバイルアプリケーションを開発するために2つの他の保健機関と緊密に連携しています。彼らは、新しいモバイルアプリケーションの結果を確認するためにパイロットを開始することに決めました。このパイロットでは、医療データに加えて、医師と患者の両方が、個人データと資格情報をモバイルアプリケーションに追加します。このパイロットのプロセスでは、セキュリティテストが実行されました。これらのテスト結果から、モバイルアプリケーションはまったく安全ではないことが判明しました。簡単にハッキングすることができ、患者のデータを変更できるような状況であり、医師の立場を乗っ取り、患者の医療情報を変更することも可能です。

3つの保健機関に指名されたデータ保護責任者(DPO)は、データ主体の利益を考慮して何をするべきでしょうか？

A) データ保護責任者(DPO)は、これがパイロットに過ぎず、患者全体のうち比較的小人数の患者が参加しているため、対応する必要はありません。
B) 検出された脆弱性の影響は、これがパイロットだけであるため、発生する可能性の高いリスクとは判断されないため、データ保護責任者(DPO)は措置を講じる必要はありません。
C) データ保護責任者(DPO)は、テスト結果は参加している患者及び医者に高いリスクをもたらす可能性が高いため、参加している患者及び医師に通知する必要があります。彼は監督当局にも通知する必要があります。
D) データ保護責任者(DPO)は、テスト報告書を使用して、セキュリティリスクをモバイルアプリケーションの必要な安全基準に合わせて調整し、監督当局にする必要があります。

A) 不正解。患者に影響する潜在的な個人データ侵害においては、患者の人数は決定的要因ではありません。発生する可能性がある高いリスクの質が決定的要因です。
B) 不正解。これがパイロットであるという事実は、発生する可能性がある高いリスクを患者に負わせる理由にはなりません。モバイルアプリケーションの実装方法とパイロットであることとの関連性はありません。
C) 正解。このテスト結果は、ハッカーがそのモバイルアプリケーションに容易に侵入できデータを改変できることから、暗号化がされていないことを示しており、管理者（コントローラ）は高いリスクが発生する事象について、不十分な対策を講じています。（文献A、第14章、段落 Notification (e-book, pg. 135, 136)）
D) 不正解。これは将来のリスクを軽減/緩和するのに役立つかもしれませんが、参加している患者や医師に対するリスクが引き続き高いため、この状況を通知する必要があります。

17 / 40
外部機関にデータ保護とプライバシー評価の実施を委託する**主要な**理由は何ですか？

A) 自社のプライバシー活動と業界標準とを比較するベンチマークテストをするため
B) 社内のプライバシーポリシーと適用される法的要件への遵守を独立した立場で検証するため
C) 自社のデータ保護およびプライバシープログラムの信頼性を向上させるため
D) 自社のデータ保護とプライバシープログラムにおいて時間と予算の制約が主要な検討事項であるため

A) 不正解。外部機関がデータ保護およびプライバシーの評価を行う理由は、社内のプライバシーポリシーと適用される法的要件の遵守を検証することです。
B) 正解。会社または組織は、社内のプライバシーポリシーと適用される法的要件の遵守を検証するために、外部のサービスプロバイダーに評価を依頼することができます。独立した外部機関は、会社のデータ保護およびプライバシー評価の実施に偏りのない視点で提供することができます。これは、外部機関が会社のシステムやプロセスに精通していないため、偏った見方や盲目的にならず、新たな視点と心で客観的に見ることができるからです。（文献B、第2.2章 Phase 5 step RI#2）
C) 不正解。データ保護とプライバシープログラムの信頼性を向上させることが、外部機関を活用する理由ではありません。データ保護とプライバシープログラムの信頼性は、完全に統合されたデータ保護及びプライバシー管理システム（DPPシステム）のすべての段階が実装された後にのみ向上させることができます。
D) 不正解。時間と予算が制約されている場合、組織は一般的に内部スタッフに依頼してデータ保護とプライバシーの評価を行います。

18 / 40
ある会社は、顧客関係管理（CRM）システムの停止を2時間以上引き起こした個人データの侵害に直面しています。この会社のデータ保護責任者（DPO）として、あなたは、とりわけアドホック的な（暫定的な）プライバシー評価を行うことを決めました。

このアドホック的な評価の**主要な**目的の一つは何ですか？

A) 顧客への適切なメッセージを助言するため
B) この侵害による被害の程度を評価するため
C) プライバシーリスクを判断するため
D) この侵害の責任者を特定するため

A) 不正解。顧客への適切なメッセージについての助言は、アドホック的な（暫定的な）評価の際に実施するのではなく、侵害の調査中に実施されるものです。
B) 不正解。被害の程度の評価は、侵害の調査中に実施されるものであり、アドホック的な（暫定的な）評価の際に実施するものではありません。
C) 正解。 プライバシー侵害の発生後にアドホック的な（暫定的な）評価を実施する目的の1つは、プライバシーリスクを特定することであり、将来同様の侵害が今後再発することを防ぎます。（文献B、段落 2.2.5, Step RI#3）
D) 不正解。この侵害の責任者の特定は、アドホック的な（暫定的な）評価の際に実施するのではなく、侵害の調査中に実施されるものです。

19 / 40
データ管理者（コントローラ）である企業は、財政難に直面しており、取締役会はデータ保護管理システム（DPMS）のソフトウェアを更新しないことに決めました。代わりに、彼らはデータ保護認証を適用するために、監督当局に承認を要求しました。これにより、会社は多くの資金を節約し、より商業的価値を高めることができます。

もしあなたがこの管理者（コントローラ）のデータ保護責任者(DPO)なら、取締役会にどのような助言をしますか？

A) データ保護認証を取得するためのプロセスを継続する。取得した認証は管理者（コントローラ）としての義務を順守していることを実証するのに使用することができます。
B) 外部のデータ保護とプライバシーの評価を実行する。これは予算を全部使うことになるが、その性質、範囲、文脈の中で適切な技術的および組織的措置が取られることを確実にします。
C) 社内評価でもっとも脆弱性が高く、更新が必要だと判明した部分だけを更新して、本来更新するべきDPMSの3分の1だけの更新を実施します。
D) DPMSへの更新を実施する。 DPMSの更新に失敗すると、管理者（コントローラ）として適切な技術的および組織的措置を講じていないとみなされる可能性があるため、遵守違反となる潜在的なリスクが発生します。

A) 正解。認証機構（メカニズム）を管理者（コントローラ）としての順守状況を実証するための要素として使うことが可能です。（文献A、第12章 Demonstrating Compliance. 文献C、第24項 subsection 3 GDPR）
B) 不正解。監督当局によって承認されたデータ保護証明書を取得するという代替方法と比較して、これは効果の低い選択肢であり、「適切」とはいえません。
C) 不正解。監督当局によって承認されたデータ保護証明書を取得するという代替方法と比較して、これは効果の低い選択肢であり、「適切」とはいえません。
D) 不正解。更新しないとしても、それ自体が違反につながるわけではありません。管理者（コントローラ）としての責任は、他のオプションが可能であることを示す「適切な」措置を取ることに基づくことです。

20 / 40
あるパリ中心部の人気フィットネスクラブは、同じくパリにあるホスティング会社にデータを保管しています。フィットネスクラブの会員のデータが保管されているサーバは最近ITサービス会社による定期点検を受けました。ITサービス会社が訪れた翌日、サーバが故障し、サーバルーム内で火事が発生しました。この火事によってフィットネスクラブのデータは喪失し、同じサーバ上に保管されていたバックアップも失われました。調査によってサーバルームの冷却システムに不具合があり、サーバシステムのオーバーヒートが発生したことが判明しました。保守エンジニアは、その室内の温度が少々高いことに気づいていましたが、急いでいたため及び、それほど異常だとは感じなかったため、このことをサーバ会社には報告しませんでした。冷却システムはホスティング会社自身のサービスに含まれます。

このインシデントに対して責任がある可能性が**最も**高いのはどの関係者ですか？

A) フィットネスクラブ。喪失したデータの所有者である組織のため
B) フィットネスクラブ。バックアップを他のサーバに保管するよう依頼しなかったため
C) ホスティング会社。個人データ周辺のセキュリティに責任があるため
D) IT会社。保守エンジニアはサーバルームの温度がかなり高いことを報告する義務があったため

A) 不正解。フィットネスクラブー管理者（コントローラ）ーフィットネスクラブはデータ取扱いの方法の要素を一つずつ定義する必要はありません。個人データ周辺のセキュリティは処理者であるホスティング会社自身に責任があります。
B) 不正解。バックアップの保管方法について指示をするのは処理者であるホスティング会社の責任です。管理者（コントローラ）であるフィットネスクラブはデータの処理方法の要素を一つずつ定義する必要はありません。
C) 正解。処理者であるホスティング会社は個人データ周辺のセキュリティに責任があります。管理者（コントローラ）であるフィットネスクラブはデータの処理方法の要素を一つずつ定義する必要はありません。（文献A、第12章、段落Data processors.）
D) 不正解。IT企業は、定温より高い温度を報告する責任はありません。これは多くの要因によって引き起こされた可能性があるからです。高温の状況に至ったのはサーバー自体から発生したわけではないため、IT会社の責任ではありません。

21 / 40
ある病院は患者の請求書の印刷を印刷会社に委託しました。印刷会社は、他の組織の請求書も印刷しています。名前と住所が印刷会社で仕分けられた際に混同されたため、間違った患者に複数の請求書が送付されました。病院は慎重に事業を分析していました。同病院は、堅牢な検証プロセスが実装されており、印刷会社とも契約上の契約を結んでいました。

印刷会社が責任を負う可能性が高いのはなぜですか？

A) 印刷会社が取扱い活動の目的を決定するため
B) 印刷会社が印刷手続を決定するため
C) 印刷会社が、どのデータを処理するかを決定するため
D) 印刷会社が他の組織の請求書を印刷しているため

A) 不正解。GDPRで規定された責任は管理者（コントローラ）と処理者にあります。病院は、処理活動の目的を決定する際の管理者（コントローラ）です。印刷会社は処理者です。 GDPRの下で、管理者（コントローラ）はデータ保護の原則を順守し、それを証明することができなければなりません。ただし、管理者（コントローラ）が損害に対して責任がないことを何らかの方法で証明できた場合、免責されることがあります。処理者が管理者（コントローラ）の適法な指示に従わない、またはそれに反する行為をした場合、処理者は責任を負うことになります。この場合病院は、その処理活動が遵守されていることを確実にするための対策を講じているため、印刷会社が責任を負う可能性が高くなります。
B) 正解。GDPRで規定された責任は管理者（コントローラ）と処理者にあります。病院は、処理活動の目的を決定する際の管理者（コントローラ）です。印刷会社は処理者です。 GDPRの下で、管理者（コントローラ）はデータ保護の原則を順守し、それを証明することができなければなりません。ただし、管理者（コントローラ）が損害に対して責任がないことを何らかの方法で証明できた場合、免責されることがあります。処理者が管理者（コントローラ）の適法な指示に従わない、またはそれに反する行為をした場合、処理者は責任を負うことになります。この場合病院は、その処理活動が遵守されていることを確実にするための対策を講じており、違う患者に請求書を送付印刷会社が責任を負う可能性が高くなります。（文献A、第12章、pg. 211-215）
C) 不正解。GDPRで規定された責任は管理者（コントローラ）と処理者にあります。病院は、処理活動の目的を決定する際の管理者（コントローラ）です。印刷会社は処理者です。 GDPRの下で、管理者（コントローラ）はデータ保護の原則を順守し、それを証明することができなければなりません。ただし、管理者（コントローラ）が損害に対して責任がないことを何らかの方法で証明できた場合、免責されることがあります。処理者が管理者（コントローラ）の適法な指示に従わない、またはそれに反する行為をした場合、処理者は責任を負うことになります。この場合病院は、その処理活動が遵守されていることを確実にするための対策を講じているため、印刷会社が責任を負う可能性が高くなります。
D) 不正解。GDPRで規定された責任は管理者（コントローラ）と処理者にあります。病院は、処理活動の目的を決定する際の管理者（コントローラ）です。印刷会社は処理者です。 GDPRの下で、管理者（コントローラ）はデータ保護の原則を順守し、それを証明することができなければなりません。ただし、管理者（コントローラ）が損害に対して責任がないことを何らかの方法で証明できた場合、免責されることがあります。処理者が管理者（コントローラ）の適法な指示に従わない、またはそれに反する行為をした場合、処理者は責任を負うことになります。この場合病院は、その処理活動が遵守されていることを確実にするための対策を講じているため、印刷会社が責任を負う可能性が高くなります。

22 / 40
ある家族経営の住宅設備の小売店は、対象を絞った広告とマーケティングのためにウェブサイト分析会社と連動することを決定しました。地元の医師と弁護士は、他のクライアントもいる同じウェブサイト分析会社と連動することを決めました。

データ保護責任者(DPO)を指名する必要があるのはどの組織ですか？

A) 家族経営の住宅設備の小売店
B) 家族経営の住宅設備の小売店とウェブサイト分析会社
C) 医師と弁護士
D) ウェブサイト分析会社

A) 不正解。ウェブサイト分析会社がデータ保護責任者(DPO)を指名する必要があります。主要な活動は、顧客に代わって個人データの処理と分析を継続的かつ大規模に行うことです。小規模な家族経営の住宅設備店や医師、弁護士による顧客の個人データの処理は、大規模な処理を構成するものではありません。
B) 不正解。ウェブサイト分析会社がデータ保護責任者(DPO)を指名する必要があります。主要な活動は、顧客に代わって個人データの処理と分析を継続的かつ大規模に行うことです。小規模な家族経営の住宅設備店や医師、弁護士による顧客の個人データの処理は、大規模な処理を構成するものではありません。
C) 不正解。ウェブサイト分析会社がデータ保護責任者(DPO)を指名する必要があります。主要な活動は、顧客に代わって個人データの処理と分析を継続的かつ大規模に行うことです。小規模な家族経営の住宅設備店や医師、弁護士による顧客の個人データの処理は、大規模な処理を構成するものではありません。
D) 正解。ウェブサイト分析会社はデータ保護責任者(DPO)を指名する必要があります。主要な活動は、顧客に代わって個人データの処理と分析を継続的かつ大規模に行うことです。小規模な家族経営の住宅設備店や医師、弁護士による顧客の個人データの処理は、大規模な処理を構成するものではありません。（文献A、第2章、 introduction and Lit. C article 37 b GDPR)

23 / 40
オランダに面する北海に浮かぶ小さな島、テッセル島に一次医療の医師がいます。彼はプライベート（利益）組織を所有しています。彼の医療行為は登録された60人に及びます。

データ保護責任者(DPO)を指名する必要があるかどうかに関して正しく記述しているのはどれですか？

A) この医療行為は、大規模な医療データと管理と取扱いを行う業務とみなすには規模が小さすぎるため、この一次医療の医師はデータ保護責任者(DPO)を指名する必要はありません。
B) 医療行為は定期的かつ体系的に患者を健診するため、医師はDPOを任命する義務があります。
C) この一次医療の医師は、この島で唯一の医療行為を行っています。彼は彼の患者に関して独立した専門的な役割を果たしています。彼は同時に医師とデータ保護責任者(DPO)の役割を兼ねることができます。

A) 正解。データ保護責任者(DPO)を指名する義務は、その性質、適用範囲、目的によって、中心的業務として大規模にデータを取扱っている、またはGDPR第9条および第10条に規定された特別な種類のデータを大規模に取扱うことに関連する中心的業務を行う公的機関や団体、または企業にのみ適用されます。（文献C、GDPR第9条及び第10 条及びGDPR第37（1）b項及びc項、文献A、第2章、序章）
B) 不正解。患者は必要があるときだけ一次医療の医師の助言を求めるだけであり、組織的に健診を受けているわけではありません。医療や健康問題の記録も大規模に実施されているわけではありません。GDPR第37条参照。
C) 不正解。この一次医療の医師は彼の患者の健康データを管理する責任があり、企業として自分の医療行為を管理しています。自分の企業の代表取締役であるこの医師は患者の個人的な健康データに関して独立した役割を持たず、そのためデータ保護責任者(DPO)にはなれません。

24 / 40
一般データ保護規制（GDPR）の下では、データ保護責任者（DPO）は、業務の実行に関する秘密または機密性に拘束されます。

データ保護責任者(DPO)がこの秘密や機密性の制約を受けずに助言を求めることができるのはどの当事者との関係においてですか？

A) 自社の取締役会
B) データ保護とプライバシーネットワークメンバのチーム
C) 情報セキュリティ責任者(ISO)
D) 監督機関

A) 不正解。容易にアクセスができるということは、データ保護責任者(DPO)が取締役会の助言を求めるべきだという意味ではありません。DPOは独立した役割を果たす必要があります。DPOの主要なタスクの一つは、管理者（コントローラ）と処理者に助言を提供することです。（文献A 、第2章 Duties of the DPO p. 49（e-book pg. 32)、文献C GDPR 第39項）
B) 不正解。容易にアクセスができるということは、データ保護責任者(DPO)がデータ保護とプライバシーネットワークメンバのチームの助言を求めるべきだという意味ではありません。DPOは独立した役割を果たす必要があります。DPOの主要なタスクの一つは、管理者（コントローラ）と処理者に助言を提供することです。（文献A 、第2章 Duties of the DPO p. 49（e-book pg. 32)、文献C GDPR 第39項）
C) 不正解。容易にアクセスができるということは、データ保護責任者(DPO)が情報セキュリティ責任者(ISO)の助言を求めるべきだという意味ではありません。DPOは独立した役割を果たす必要があります。DPOの主要なタスクの一つは、管理者（コントローラ）と処理者に助言を提供することです。（文献A 、第2章 Duties of the DPO p. 49（e-book pg. 32)、文献C GDPR 第39項）
D) 正解。守秘義務によってDPOが監督機関に連絡をしたり助言を求めたりするのが制約されることはありません。（文献D、段落4.3）

25 / 40
あなたはある高級ファッションの百貨店チェーンでデータ保護責任者(DPO)として雇用されています。同社は、正規の顧客を識別してより良いサービスを提供するために、顔認識ソフトウェアを購入する意向を表明しています。アカウントを保持しているすべての顧客にこの変更が通知され、オプトアウトの選択肢が提供される予定です。

データ保護影響評価(DPIA)を事前に実施することをあなたが推奨すべき理由はどれですか？

A) ISO27001によると、DPIAは情報セキュリティマネジメントシステム(ISMS)の必須項目であるため
B) DPIAを実施し、経営陣による承認を得て、将来のセキュリティインシデントに対する責任を負う可能性をなくすことはグッドプラクティス（良い慣行）の一環であるため
C) GDPRでは、プロファイリングや大量のモニタリングを通じて、個人情報の保護に影響を与える可能性のある新しい技術が使用される場合、DPIAが必須であると規定しているため
D) GDPRでは、現行のプロセス、プロジェクト、またはポリシーの変更に対してDPIAは必須であると規定しているため

A) 不正解。ISO27001は一般的なセキュリティに適用されるものであり、DPIAの必要性については言及していません。
B) 不正解。組織はIT戦略に起因するいかなるインシデントについても、責任を負う可能性があり、実際に負うことになります。DPIAは、関連するリスクを指摘するのに役立つだけです。
C) 正解。DPIAは、新技術を組み込む際には一般的にはグッドプラクティス（良い慣行）と見なされますが、3つの条件が揃えば必須とみなされます。百貨店は、公的にアクセス可能な領域であり、視覚的な電子機器を使用して体系的に監視されることになります。自動プロファイリングは、特定の自然人に関して特定するために使用されます。この場合、少なくとも3つの条件のうち2つが適用されます。（文献A、第5章 1. Identify the need for a DPIA）
D) 不正解。DPIAはGDPRで常に必須とは限りません。

26 / 40
あなたは、大規模な組織で働いているとします。あなたの所属する組織は、コンピュータ上の作業に関する従業員の監視を容易にするソフトウェアツールを使用しています。これらのツールは、一般的なアルゴリズムと時間を示す指標に基づいて、休憩やストレッチが必要なタイミングを示します。休憩時間についての助言をより適切にパーソナライズするために、監視ツールを心拍計に接続することで機能性を追加することが発案されました。

DPIAを実施しなければならない理由はどれですか？

A) 新しいツールやプロセスにはDPIAが必須であるため
B) このツールは従業員を監視することにより個人データの取扱いを含むようになるため
C) これは機微な個人データの処理を含む新しいアプリケーションであるため
D) これは公的な場における大規模な行動観察を含む新しいアプリケーションであるため

A) 不正解。既存のツールやプロセスに追加する新しいアプリケーションや機能については、常にDPIAが必須であるとは限りません。
B) 不正解。従業員の個人データを処理するという事実だけではDPIAを必要とする理由としては不十分です。
C) 正解。GDPRに記載されている、DPIAに関する第35条には、機微な個人データを大規模に処理する場合はDPIAを実施しなければならないと示されています。健康に関するデータは機微データです。（文献A、第5章、段落When to conduct a DPIA?（e-book pg. 62-63）、文献C: GDPR 第3部、第35条(3)b および9(1)）
D) 不正解。これもGDPRに記載された根拠ですが、この場合は公的空間ではないので適用されません。

27 / 40
あなたは、運輸省（Ministry of Transportation）最高プライバシー責任者として新しい仕事を始めました。新しく国道の人々の運転行動を監視するためのプロジェクトが発表されました。同部では知的なビデオ分析システムを使用して車を選別し、ナンバープレートを自動的に認識することを想定しています。ある朝、国務長官があなたのオフィスを訪れました。長官は明らかにプロジェクトの開始を急いでいるようで、プライバシー問題によって望ましくない遅れが引き起こされるかもしれないという懸念を明らかにしました。

あなたは長官に何を言うべきですか？

A) これは、自分の権限をはるかに上回る国家的にも重要な課題であることから、監督機関に連絡をとることを長官に依頼する
B) 想定されているデータ取扱いの性質はDPIAによる精査を要求するものであることを長官に伝える。生じるリスクと緩和対策をプロジェクト計画に組み込む必要がある
C) 国民に処理活動の目的と範囲について適切に通知している限り、DPIAの必要がないことを長官に通知します。
D) GDPRでは大規模な監視やプロファイリングなどの「高リスク」なデータ処理業務が禁止されているため、プロジェクトは真剣に再考をするべきだと長官に伝える

A) 不正解。あなたは最高プライバシー責任者であり、プライバシーに関する省レベルの課題を話し合う資格は十分にあるはずです。
B) 正解。このプロジェクトには、技術的ソリューションの革新的な使用と同様に、体系的な監視が必要となります。DPIAを実施する3つの理由のうちの2つを満たしています。（文献A、第5章 Identify the need for a DPIA, When to conduct a DPIA）
C) 不正解。適切な通知をしたとしても、組織は、個人データの保護に関して想定される処理業務の影響を評価する責任を免除されることはありません。
D) 不正解。人々の権利と自由が十分に保護されている限り、モニタリングと監視はそれ自体禁止されていません。

28 / 40
GDPRは特定の条件下でデータ保護影響評価(DPIA)を実施する必要があることを規定していますが、実際*どのように*実施するかについては記述していません。それでも、GDPRはDPIAから得られる望ましい成果の最小限のセットを明確に特定しています。

この最小限の望ましい成果を考慮した場合、**常に**DPIAに含まれるべき活動はどれですか？

A) データ主体の権利を保護するため、主体によるアクセス要求手続を開発する
B) 処理される個人データと処理の目的を識別する
C) データ主体に分析が実施されることを通知し、明確な同意を要求する
D) インシデント対応計画を作成し、データ侵害を回避する適切な保護措置を定義する

A) 不正解。これはDPIAの成果となりえる対策です。が、DPIAの標準的な段階や活動ではありません。
B) 正解。データマッピングは、すべてのDPIAに不可欠です。収集と処理を行っている個人データを識別し理解するところから始まります。（文献A、第8章 Objectives and outcomes, Five key stages of the DPIA）
C) 不正解。DPIAに関してはデータ主体との同意は必要ではありません。DPIAは個人データに対するリスクを増加させるものではなく、リスクの分析と軽減を目的としています。
D) 不正解。データ侵害に関する適切な対応戦略を定義するのはDPIAの成果となりえる対策です。が、DPIAの標準的な段階や活動ではありません。

29 / 40
ある会社は、トレンドを検知・分析し、予測を改善できるように顧客データをより有効に活用することを決定しました。新たな組織的ユニットが設立される予定です。データの専門家は最新のデータ分析ツールを使ってデータウェアハウスを構築する予定です。

データ保護責任者(DPO)の役割を持つあなたは、このことがデータ主体の権利に悪影響を及ぼす高リスクな試みであると深い懸念を示しました。しかし、CIOとCEOの両方が開発を進めることを望んでおり、あなたの懸念に対応することには消極的です。

とるべき行動として**最適**なのはどれですか？

A) DPIAを実施し、取締役会及びその他の利害関係者とDPIAの結果及び可能な緩和策について議論する
B) CIOにデータの匿名化を関与させることによりGDPRが適用されないようにする
C) 顧客に相談し、現行の処理について明示的な同意を求める顧客アンケートを設定する
D) 監督機関に連絡し、意図している処理について見解を求め、リスク説明についての助言を依頼する

A) 正解。最初にするべきことは含まれるリスクの評価です。リスクが高い場合は、その企業の「リスク選好」に基づいてリスクを軽減する対策をとることができます。（文献A、第8章、段落Consultation and 第5章、段落Privacy impact assessments, step 1. Identify the need for a PIA and paragraph When to conduct a DPIA）
B) 不正解。データの匿名化または仮名化はリスク軽減対策となり得ますが、まずはDPIAを実施しリスクを決定する必要があります。さらに、データの匿名化も処理活動であるため、データの匿名化を行う正当な事由が必要となります。
C) 不正解。明確な同意は、目的の制限やデータの最小化などのプライバシーの原則に違反する処理業務を正当化しません。
D) 不正解。最初にリスクを評価することです。リスクが低い場合、またはリスクを低減するために十分な措置を講じることができる場合は、監督当局（DPA）に連絡する必要はありません。

30 / 40
なぜデータ保護影響評価（DPA）は組織のリスク管理の一環とみなされるのでしょうか？

A) DPIAは、その組織が軽減しなければならないデータ主体のリスクを識別するものであるため
B) DPIAは、その組織が軽減しなければならない組織のセキュリティリスクを識別するものであるため
C) DPIAは、リスクを分類するために必要な影響を測定するものであるため
D) DPIAは、組織がGDPRを順守するのに必要であるため

A) 正解。文献A、第6章、段落DPIAs as part of risk management参照。
B) 不正解。DPIAは個人データ保護への影響を重視します。
C) 不正解。これはリスクが「影響×確率」で算出される情報セキュリティのアプローチですが、DPIAの目的ではありません。ただし、DPIAの結果は潜在的なリスクと影響に従って軽減される可能性があります。
D) 不正解。DPIAは常に必須ではなく、新しい処理活動や技術または高いリスクがある場合にのみ必要となります。GDPR第35条参照。したがって、DPIAを実施しなくてもGDPRを順守することが可能です。

31 / 40
データ保護影響評価(DPIA)では、プライバシーに対するリスクを特定することが重要です。次の段階では、これらのリスクを排除するか、受容レベルまで軽減することです（リスク対応）。

典型的なリスク対応を構成するのはどの行動ですか？

A) 有効性の指標を定義する
B) 収集したデータの量を削減する
C) プライバシーリスクの登録を設定する
D) DPIAの結果を承認し、記録する

A) 不正解。これはリスクを緩和する対応ではありません。
B) 正解。これは、データ侵害の潜在的な影響を軽減するための重要なリスク対応を示しています。（文献A、第8章、Five key stages of the DPIA）
C) 不正解。これはリスクを緩和する対応ではありません。
D) 不正解。これはリスクを緩和する対応ではありません。

32 / 40
データ保護インパクトアセスメント（DPA）を実施する必要がある場合、GDPRにはいくつかの要素が必要となります。これらの要素のうちの2つは、比例原則と必要性の評価及び特定されたリスクを緩和するための対策の評価です。

GDPRの規定によってDPIAに含める必要がある他の要素はどれですか？

A) データ侵害の対処方法に関する手順
B) DPIAの結果に関する公式報告書（公表）
C) データ主体に及ぼすプライバシーに関するリスクの評価

A) 不正解。データ侵害の手順について形式張る必要はなく、あるとしても、それはDPIAの一部ではありません。
B) 不正解。GDPRでは、結果に関する公式報告書（公表）を要求していません。（文献A、第8章Five key stagesに記述がありますが）。
C) 正解。この要素は以下に記述されています。文献C: GDPR第3部、第35(7) 条。文献A、第5章 Privacy Impact Assessments及び第8章Five key stages of the DPIA。文献E: 第III章、段落C How to carry out a DPIA?

33 / 40
あなたは、個人データの処理を含む組織内のプロジェクトに対して責任を負います。責任の一部として、データ保護影響評価（DPA）を実行し、データマッピングを開始することを決定しました。

DPIAプロセスにおいてデータマッピングが役立つ理由はどれですか？

A) 個人データに対するリスクの概要を得るのに役立つため
B) データ処理に用いられるシステムの概要を得るのに役立つため
C) 処理の目的を識別するのに役立つため

A) 正解。文献A、第7章Data mapping, DPIAs and risk management及び文献C、GDPR第35(1)条。
B) 不正解。これは必要な処理の記録に含まれます（GDPR第30条）。
C) 不正解。これはDPIAを実施する前に決定すべきであり、データマッピングから得られるものではありません。

34 / 40
ある組織は、プロファイリングに基づいて顧客に対して自動化された意思決定を行う予定です。

データ保護影響評価(DPIA)のプロセスのうち、特に注意を払うのに**最も適した**側面はどれですか？

A) この処理活動に関連してDPIAを実行する必要性の評価
B) データがいつ消去されるかの評価
C) 人の介入を促進することによってデータ主体の権利を保護するための対策
D) データを保護し、データ主体がデータにアクセスできないようにするための対策

A) 不正解。プロファイリングを含む自動化された意思決定を伴う処理活動については、DPIAが常に必要となります。（GDPR、第35(3) a条）。DPIAを実施する必要があります。
B) 不正解。これはDPIAプロセスの一部ですが、この場合では特に注意する必要はありません。しかし、意義や紛争がある場合、自動化された意思決定のチェックを容易にするために、データの長期保存が必要な場合があります。
C) 正解。文献 E: 第III章、段落C How to carry out a DPIA? 、及び、文献C、GDPR、第22(3)条によって必須と規定されています。文献A、第5章、Privacy Impact Assessments and When to conduct a DPIA。
D) 不正解。データは一般的に保護される必要がありますが、データ主体にはアクセスする権利があります。（GDPR、第15条）。

35 / 40
あなたは、組織内でデータ保護影響評価(DPIA)の責任を負っています。このDPIAに伴って、想定される処理活動と目的について適切な記述を作成するために、あなたは多くの同僚と話し合いました。この協議の間、処理には現在の目的には厳密には必要ではないが、将来の目的のために使用できる個人データの収集を含むことが判りました。収集を現在のプロセスに合わせる方が効率が上がります。

あなたはこの状況で何をすべきですか？

A) GDPRの第6条に示すように、効率性は組織の正当な利益であるため、その処理を許可します。
B) DPIAが実行される処理の目的に必要でないため、追加データを収集しないことを要求します。
C) その追加データの処理に関してGDPRの第6条に則った正当な事由を示すよう同僚に要求し、取扱いを許可します。
D) データ侵害を防止するため、そのデータが適切に保護されることを要求します。

A) 不正解。正当な利益は取扱いの正当な事由になり得ますが、依然として具体的かつ明示的な目的が必要です。
B) 正解。これは個人データ処理の必要性及び比例原則の確認に則しています。文献E、第III章、段落C How to carry out a DPIA? 、文献C、GDPR第35(7)b条。追加：文献A、第5章 Introduction及び第8章 Objectives and outcomes.
C) 不正解。特定された明確な目的にだけ個人データの処理が認められます（GDPR第5条(1)b）。GDPR第6条に記載の通り、この目的が提示されていなければ、処理には正当な事由がない可能性があります。
D) 不正解。個人データの違法な処理は、それ自体がデータ侵害です。

36 / 40
あなたは会社が提供する新しいサービスのためにDPIAを実行しています。このサービスでは必然的に顧客の個人データの大規模処理を必要とします。処理には正当な理由と目的があり、関連するデータ主体の権利に対するリスクを軽減するための適切な措置が実施される予定です。しかし、サービスが成功するためには、顧客による受け入れが重要であることは明らかです。

この場合、データ保護影響評価(DPIA)プロセスを完了するのに必要となる具体的な行動はどれですか？

A) 顧客またはその代理人に相談して、個人データの処理に関する意見を求める。
B) 処理の適法性について確認をとるためにデータ保護機関(DPA)に相談する
C) ヘルプデスクを開設し、サービスを公表後、顧客がそのサービスについて説明を受けられるようにする。
D) 顧客にDPIA報告書（データ保護影響評価報告書）を送り、対策がとられることを保証する

A) 正解。文献C、GDPR、第35条(9)。文献A、第8章、段落Consultation。
B) 不正解。データ保護機関(DPA)は顧客を代表するものではなく、また、単なる合法性は、合意を意味するものではありません。
C) 不正解。これはデータ保護影響評価(DPIA)プロセスには含まれません。
D) 不正解。これは、DPIAプロセスの一部ではなく、いかなる場合でも必須項目です。

37 / 40
あなたは、国際的な顧客を持つ大規模な物流会社のデータ保護責任者（DPO）としての責任を負います。35人の従業員の人事情報を含む暗号化されたメモリースティックを紛失したか、置き忘れたと人事部門長が報告してきました。

一般データ保護規則（GDPR）において、これをデータ侵害として監督機関に報告する必要があるのはなぜですか？

A) 機密性の高い会社データの損失を伴うセキュリティインシデントは、データ侵害として報告する必要があります。
B) 個人データが含まれたデバイスの紛失は自然人の権利及び自由に対するリスクであるため、このインシデントは報告する必要があります。
C) 監督機関が35人の従業員に侵害があったことを通知できるよう、このインシデントは不当な遅滞なしに報告される必要があります。

A) 不正解。GDPRの定義によると、*個人データ*を含むセキュリティインシデントだけが、データ侵害に属します
B) 正解。デバイスの紛失は脆弱性を表しています。デバイスは十分に保護されていますが、悪意（脅威）に対して、データが危険にさらされるリスクがあります。これは、監督当局に報告する必要のあるデータ侵害となります。（文献A、第3章 Anatomy of a data breach、第14章 Notification）
C) 不正解。監督機関には、関連する利害関係者にインシデントを報告する責任はありません。

38 / 40
組織がデータ侵害を監督当局に報告する必要があるのは、どのような場合ですか？

A) インシデントが自然人の権利と自由に対するリスクをもたらす可能性がある場合すべて
B) 自然人の権利と自由を危険にさらすキュリティ上の脅威がある場合すべて
C) インシデント発生後72時間以内に組織がそのインシデントを解決できない場合のみ
D) インシデント発生後72時間以内にインシデントが認識された場合のみ

A) 正解。個人データを含むインシデントについては監督機関に通知する必要があります。（文献A、第14章、段落Notification）
B) 不正解。脅威自体だけでは十分ではありません。例えば。フィッシングは一般的な脅威と考えることができます。ただし、実際のインシデントの形で脆弱性が存在する場合にのみ、監督当局への通知が必要となります。
C) 不正解。インシデント解決によって監督機関への報告の遅滞が起きてはなりません（不当な遅滞の禁止）。
D) 不正解。インシデント管理プロセスは、72時間以内にリスクを特定できない場合があります。それよりも時間がかかることがあります。GDPRが「不当な遅滞なしに、可能であれば、侵害に気が付いてから72 時間以内に」と規定しているのはこれが理由です。

39 / 40
組織が関係するデータ主体にデータ侵害を報告する必要があるのはどのような状況ですか？

A) データ侵害が自然人の権利と自由に対する「高いリスク」をもたらす可能性がある場合すべて
B) 関係するデータ主体の権利と自由を危険にさらすセキュリティインシデントが発生した場合すべて
C) データ主体にデータ侵害を通知する必要があると監督機関が判断した場合のみ
D) サイバー犯罪者などの外部の犯行者によって個人データが危険にさらされる「悪意」が存在する場合のみ

A) 正解。個人データの侵害が自然人の権利と自由に対して「高いリスク」を課す場合にはデータ主体に通知する必要があります。（文献A、第14章 Notifications）
B) 不正解。データ主体への通知は、「高いリスク」を伴うセキュリティインシデントの場合にのみ必要があります。
C) 不正解。組織は、セキュリティ違反が発生したことをデータ主体に通知すべきかどうかを決定する際に、会社とデータ主体の利益を慎重に調整する必要があります。
D) 不正解。通知は、発生源や侵害の意図に依存しません。個人データの侵害は実際、悪意ある行動から生まれることもありますが、偶発的に生まれることもあります。

40 / 40
すべての組織は、監督当局に通知されなければならないデータ違反を処理する必要があります。通知プロセスは繰り返されるため、以下のような要素を含む報告書のテンプレートを設定することが推奨されます。

・個人データ侵害の性質
・侵害によって起こりうる影響
・緩和するための対策

このテンプレートに追加すべき項目はどれですか？

A) ・CEO の名前と連絡先の詳細
・インシデント対応計画
B) ・影響を受けるデータ被験者の名前
・侵害の責任者の名前
C) ・影響を受けるデータ主体の人数
・データ保護責任者(DPO)の名前と連絡先の詳細
D) ・セキュリティインシデントの件数
・サイバーセキュリティの脅威分析

A) 不正解。CEOは、監督当局に対するデータ侵害の通知に関与しません。インシデント対応計画も、報告すべき要素ではありません。インシデント対応計画は、監査時に監督当局によってのみ評価されることがあります。
B) 不正解。監督当局は、事件に関与した者やインシデントの影響を受けた者の名前には関心がありません。通知処理の結果により、懲罰行為が生じることはありません。
C) 正解。これらは監督機関への通知に含めなければならない項目です。（文献A、第14章 Notification）
D) 不正解。これらは報告する必要のない項目です。

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

EXIN の連絡先

www.exin.com

YOUR ICT COMPETENCE PARTNER