Exemple d'examen

Édition 201803

Table des matières

Introduction	4
Exemple d’examen	5
Solutions de l’examen	17
Évaluation	38

Introduction

Voici l’exemple d'examen EXIN Privacy & Data Protection (PDPF.FR). Les règles et réglementations d'examens EXIN s'appliquent à cet examen.

Cet examen consiste en 40 questions à choix multiples. Chaque question à choix multiple comporte un certain nombre de réponses possibles dont seulement une est correcte.

Le maximum de points qui peut être obtenu lors de l'examen est de 40. Chaque réponse correcte rapporte un point. Si vous obtenez 26 points ou plus vous réussissez votre examen.

Le temps alloué lors de l'examen est de 60 minutes.

Bonne chance !

Exemple d'examen

1 / 40
La collecte, le stockage, la modification, la divulgation ou la diffusion illégale de données personnelles est une infraction au droit européen.

De quel type d'infraction s'agit-il ?

A) Une infraction relative au contenu
B) Une infraction d'ordre économique
C) Une infraction à la propriété intellectuelle
D) Une infraction à la protection des renseignements personnels

2 / 40
Quel est le rapport entre la protection de la vie privée et la protection des données ?

A) La protection des données fait partie de la protection de la vie privée.
B) La protection de la vie privée fait partie de la protection des données.
C) Il s'agit de la même chose.
D) La protection de la vie privée ne peut être réalisée sans protection des données.

3 / 40
À quoi est **principalement** destiné le Réglement Général de Protection des Données (RGPD) ?

A) À servir de base commune sur laquelle les états membres peuvent élaborer leurs propres lois
B) À faire en sorte que les pays non membres de l'UE respectent le droit à la vie privée des individus au sein de l'UE
C) À garantir la protection des renseignements personnels en tant que droit fondamental de chaque être humain
D) À renforcer et unifier la protection des données des individus au sein de l'UE

4 / 40
Le Réglement Général de Protection des Données (RGPD) a trait à la protection des données personnelles.

Quelle est la définition des données personnelles ?

A) Toute information concernant une personne physique identifiée ou identifiable
B) Toute information que les citoyens européens souhaitent protéger
C) Les données qui révèlent, directement ou indirectement, l'origine raciale ou ethnique, les convictions religieuses d'une personne, et les données relatives à sa santé ou à ses habitudes sexuelles
D) Préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information

5 / 40
Selon le Réglement Général de Protection des Données (RGPD), quelle catégorie de données personnelles est considérée comme des données sensibles ?

A) Les informations de carte de crédit
B) L'appartenance à un syndicat
C) Le numéro de passeport
D) Le numéro de sécurité sociale

6 / 40
Selon le Réglement Général de Protection des Données (RGPD), quelle est la définition du "traitement" de données personnelles ?

A) Toute opération qui peut être effectuée sur des données personnelles
B) Toute opération qui peut être effectuée sur des données personnelles à l'exception de leur effacement et de leur destruction
C) Uniquement les opérations au cours desquelles les données sont partagées sur les médias sociaux ou transférées par courriel ou par tout autre moyen utilisant Internet
D) Uniquement les opérations dans lesquelles les données personnelles sont utilisées aux fins pour lesquelles elles ont été recueillies

7 / 40
"Une autorité publique indépendante qui est établie par un état membre conformément à l'article 51."

De quel rôle dans la protection des données est-ce la définition ?

A) Responsable du traitement
B) Sous-traitant
C) Autorité de contrôle
D) Tiers

8 / 40
En vertu du Réglement Général de Protection des Données (RGPD), un 'consentement éclairé' constitue une base légale du traitement des données personnelles. L'objectif du traitement pour lequel le consentement est donné doit être documenté.

À quel moment dans le processus, le consentement de la personne concernée doit-il être obtenu ?

A) Après que les caractéristiques de la finalité aient été communiquées et avant la collecte des données personnelles
B) Avant que les caractéristiques de la finalité ne soient élaborées et présentées
C) Avant le traitement des données personnelles
D) Avant la publication ou la diffusion des données personnelles

9 / 40
Le principe de proportionnalité et de subsidiarité constitue l'une des bases du Réglement Général de Protection des Données (RGPD).

Quel est le sens de la 'proportionnalité' dans ce contexte ?

A) Les données personnelles peuvent uniquement être traitées conformément aux caractéristiques de la finalité.
B) Les données personnelles ne peuvent pas être réutilisées sans un consentement explicite et éclairé.
C) Les données personnelles ne peuvent être traitées que dans le cas où il n'existe pas d'autres moyens d'atteindre les objectifs.
D) Les données personnelles doivent être adéquates, pertinentes et non excessives au regard des finalités.

10 / 40
Le traitement des données personnelles doit répondre à certains critères de qualité.

Quel est l'un de ces critères de qualité définis par le Réglement Général de Protection des Données (RGPD) ?

A) Les données traitées doivent être archivées.
B) Les données traitées doivent être encodées.
C) Les données traitées doivent être indexées.
D) Les données traitées doivent être pertinentes.

11 / 40
Chaque fois que des données personnelles sont traitées, il convient de vérifier la proportionnalité et la subsidiarité.

Quelles sont les exigences applicables aux données personnelles traitées ?

A) Elles doivent toujours être limitées au strict nécessaire permettant d'atteindre les objectifs définis et aux données les moins "intrusives".
B) Elles doivent être manipulées par le nombre le plus restreint possible d'employés et ces derniers doivent travailler pour le responsable du traitement ou une filiale.
C) Elles doivent être limitées à une taille de stockage prédéfinie et le système utilisé doit être financé par le responsable du traitement.
D) Elles doivent être utilisées pour le plus petit nombre de buts possible et leur utilisation doit rester confinée aux locaux du sous-traitant.

12 / 40
"Le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour veiller à ce que (...) seules soient traitées les données personnelles nécessaires à chaque objectif."

De quel terme du Réglement Général de Protection des Données (RGPD) est-ce la définition ?

A) Conformité
B) Protection des données par défaut
C) Protection des renseignements personnels dès la conception
D) Protection intégrée

13 / 40
Quel est le terme utilisé dans le Réglement Général de Protection des Données (RGPD) pour une divulgation de données personnelles ou un accès non autorisés à ces dernières ?

A) Violation de confidentialité
B) violation de données
C) Incident
D) Incident de sécurité

14 / 40
Il a été établi qu'une violation de données personnelles sensibles s'est produite.

D'après le Réglement Général de Protection des Données (RGPD), à qui cela doit être signalé en dernier ressort ?

A) L'autorité de contrôle
B) Le délégué à la protection des données (DPO)
C) Le responsable du service
D) La police

15 / 40
Le disque d'un serveur de données se plante lors d'une sauvegarde. Les données et la sauvegarde sont perdues. Le disque contenait des données personnelles mais pas de données sensibles.

De quel genre d'incident s'agit-il ?

A) Violation de données
B) Violation de sécurité
C) Incident de sécurité

16 / 40
Une personne travaillant pour un syndicat a emporté chez elle un projet de bulletin d'information à envoyer aux membres pour finir d'y travailler. La clé USB contenant le projet et la liste de diffusion, a été perdu.

À qui, entre autres, cette violation de données devrait-elle être signalée ?

A) Tous les membres sur la liste de diffusion
B) Le personnel du syndicat
C) La police

17 / 40
Un organisme de services sociaux prévoit de concevoir une nouvelle base de données pour gérer ses clients et les soins dont ils ont besoin.

Quelle est l'une des premières mesures importantes à prendre en vue de demander l'autorisation à l'autorité de contrôle ?

A) Recueillir des données sur les clients ainsi que sur la quantité et le type de soins requis et fournis.
B) Effectuer une analyse d'impact relative à la protection des données (DPIA) pour évaluer les risques du traitement prévu.
C) Obtenir le consentement des clients pour le traitement de leurs données personnelles.

18 / 40
Dans quel cas, les personnes concernées devraient-elles toujours être informées d'une violation de données ?

A) Lorsque les données personnelles ont été traitées dans les locaux d'un sous-traitant qui ne sont pas situés à l'intérieur des frontières de l'Union Européenne
B) Lorsque les données personnelles ont été traitées par une partie qui a donné son accord sur un projet de contrat avec le responsable du traitement mais n'a pas encore signé le contrat
C) Lorsque le système sur lequel les données ont été traitées a subi une attaque endommageant ses unittés de stockage
D) Lorsqu'il y a une probabilité significative que la violation ait des conséquences négatives sur la protection de la vie privée des personnes concernées

19 / 40
Un responsable de traitement a confié un contrat de traitement de données personnelles sensibles à un sous-traitant dans un pays d'Afrique du Nord, sans consulter l'autorité de contrôle. Une fois découvert, il fut pénalisé par l'autorité de contrôle. Six mois plus tard l'autorité constate que le responsable du traitement se rend coupable de la même faute pour une autre opération de traitement.

Quelle est la peine maximale que l'autorité de contrôle peut imposer dans ce cas ?

A) € 750 000
B) €1 230 000
C) € 10 000 000 ou 2% du chiffre d'affaires mondial annuel de l'entreprise, la pénalité la plus importante étant appliquée
D) € 20 000 000 ou 4% du chiffre d'affaires mondial annuel de l'entreprise avec un minimum de 20 000 000 €, la pénalité la plus importante étant appliquée

20 / 40
Les Autorités de Contrôle assument un certain nombre de responsabilités visant à s'assurer que la réglementation sur la protection des données est respectée.

Qu'est ce qui constitue l'une de ces responsabilités ?

A) L'évaluation des codes de conduite pour des secteurs spécifiques en matière de traitement de données personnelles
B) La définition d'un ensemble minimum de mesures à prendre afin de protéger les données personnelles
C) Enquêter sur toutes les violations de données dont elles ont été averties
D) L'évaluation de la conformité aux réglementations des contrats et des règles d'entreprise contraignantes

21 / 40
Une association religieuse veut partager des données personnelles avec leur autorité religieuse dans un pays non européen afin de répondre à une demande du gouvernement concerné.

Quelle est la réglementation du Réglement Général de Protection des Données (RGPD) applicable dans ce cas ?

A) À titre exceptionnel, une association religieuse est autorisée à traiter des données sensibles révélant les croyances religieuses.
B) Il est illégal de transférer des données personnelles hors de la zone Économique Européenne en réponse à une exigence légale d'un pays tiers.
C) Le traitement est licite si le consentement spécifique et non équivoque de la personne concernée a été acquis.
D) Le traitement de données personnelles en dehors de la zone économique européenne est autorisé si les clauses du contrat modèle conçu par la Commission de l'UE ont été utilisées.

22 / 40
Le 12 juillet 2016, la Commission européenne a mis en œuvre un arrêté concernant le transfert de données personnelles avec les États-Unis (EU-US Privacy Shield).

En termes de Réglement Général de Protection des Données (RGPD), de quel type d'arrêté s'agit-il ?

A) Une décision d'adéquation
B) Un décret d'exception
C) Un contrat contraignant standard
D) Un traité remplaçant le RGPD

23 / 40
Pour les entreprises, les règles d'entreprise contraignantes sont un moyen d'alléger leur fardeau administratif en vue de se conformer au Réglement Général de Protection des Données (RGPD).

De quelle manière ces règles les aident-elles ?

A) Elles leur permettent de disposer de contrats de sous-traitance avec toutes les parties concernées à l'étranger.
B) Elles leur permettent de confier le traitement de données personnelles à des tiers hors zone économique européenne.
C) Elles permettent de ne plus avoir à démarcher séparément chaque autorité de contrôle au sein de l'UE.
D) Elles permettent aux entreprises de ne plus avoir à demander l'autorisation de traiter des données à une autorité de contrôle, une fois que leurs règles contraignantes ont été acceptées.

24 / 40
Si une entreprise externalise le traitement des données personnelles, les parties passent un contrat écrit. Ce contrat décrit l'objet et la durée du traitement, la nature et le but du traitement, le type de données personnelles et les catégories de personnes concernées par les données.

Quel autre aspect doit être régi par ce contrat écrit ?

A) La responsabilité du sous-traitant
B) L'obligation de notification des violations de données
C) L'obligation du sous-traitant de coopérer avec l'autorité de contrôle
D) Les droits et obligations du responsable du traitement

25 / 40
Que faut-il entreprendre pour qu'un responsable du traitement soit en mesure d'externaliser le traitement de données personnelles auprès d'un sous-traitant ?

A) Le responsable du traitement doit demander à l'autorité de contrôle l'autorisation d'externaliser le traitement des données.
B) Le responsable du traitement doit demander à l'autorité de contrôle si le contrat écrit convenu est conforme à la réglementation.
C) Le responsable du traitement et le sous-traitant doivent rédiger et signer un contrat écrit garantissant la confidentialité des données.
D) Le sous-traitant doit montrer au responsable du traitement que toutes les exigences convenues dans le contrat de niveau de service (SLA) sont remplies.

26 / 40
La protection des données dès la conception, telle que définie à l'article 25 du RGPD est basée sur sept principes clés. L'un d'eux est généralement appelé *'Functionality – Positive-Sum, not Zero-Sum'*.

Quelle est l'essence de ce principe ?

A) Les normes de sécurité appliquées doivent assurer la confidentialité, l'intégrité et la disponibilité des données personnelles tout au long de leur cycle de vie.
B) Si différents types d'objectifs légitimes sont contradictoires, les objectifs visant la protection des renseignements personnels doivent être prioritaires sur les autres objectifs de sécurité.
C) Lors de l'intégration de la protection des renseignements personnels dans une technologie, un processus ou un système donné, cela devrait être fait de manière à ne pas entraver les fonctionnalités.
D) Dans la mesure du possible, il convient de mener une évaluation détaillée de l'impact sur et des risques pour la protection des renseignements personnels, de la publier et de documenter clairement les risques pour la protection des renseignements personnels.

27 / 40
Souvent, le personnel travaillant avec des données personnelles considère leur protection et la sécurité de l'information comme deux sujets distincts.

Pourquoi est-ce une erreur ?

A) La protection des renseignements personnels ne peut être garantie sans l'identification, la mise en œuvre et le suivi de mesures de sécurité adéquates de l'information.
B) L'autorité de contrôle s'attend à ce que les rôles de délégué à la protection des données et de chargé de la sécurité de l'information soient intégrés.
C) Les règlementations identifient des mesures spécifiques de sécurité de l'information qui doivent être prises avant d'autoriser le traitement des données personnelles.

28 / 40
L'un des objectifs d'une analyse d'impact relative à la protection des données (DPIA) est de "renforcer la confiance des clients ou des citoyens dans la façon dont les données personnelles sont traitées et la protection des renseignements personnels est respectée".

Comment une DPIA peut-elle "renforcer la confiance" ?

A) L'organisation minimise le risque de coûteux ajustements au sein de processus ou de restructuration de systèmes à un stade ultérieur.
B) L'organisation évite la non-conformité au RGPD et minimise le risque d'amendes.
C) L'organisation démontre qu'elle prend la protection des renseignements personnels au sérieux et qu'elle vise la conformité au RGPD.

29 / 40
Quel est le but d'un audit sur la protection des données par l'autorité de contrôle ?

A) S'acquitter de l'obligation imposée par le Réglement Général de Protection des Données (RGPD) consistant à mettre en œuvre des mesures techniques et organisationnelles appropriées pour la protection des données
B) Assurer l'application du RGPD en vérifiant que le traitement a lieu conformément à ce dernier
C) Conseiller le responsable du traitement quant à l'atténuation des risques sur la protection des renseignements personnels, afin de protéger le responsable du traitement de toute action en responsabilité pour non-conformité au RGPD

30 / 40
Qu'est-ce qui décrit le **mieux** le principe de minimisation des données ?

A) Il convient de recueillir le moins de données possible afin de protéger les renseignements personnels et les intérêts des personnes concernées par les données.
B) Les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
C) Pour faire en sorte que les données restent gérables, il convient de les stocker de manière à ce qu'elles nécessitent un minimum d'espace de stockage.
D) Le nombre d'éléments collectés pour chaque personne concernée ne doit pas dépasser la limite supérieure stipulée par l'autorité de contrôle.

31 / 40
Les cookies de session sont l'un des types de cookies les plus communs.

Qu'est-ce qui décrit le **mieux** un cookie de session ?

A) Il contient des informations sur ce que vous faites, par exemple les produits que vous sélectionnez dans une boutique en ligne, avant de finaliser votre commande.
B) Il révèle l'historique de votre navigation, de sorte que d'autres sites web peuvent identifier les sites web que vous avez visités avant d'arriver là où vous êtes actuellement.
C) Il enregistre l'historique de votre navigation, afin de vous permettre de conserver la trace des sites visités et d'y revenir si vous le souhaitez.
D) Il recueille vos données personnelles, permettant au site web de vous saluer par votre nom et de réutiliser vos paramètres lorsque vous revenez.

32 / 40
Parfois certains sites web suivent les visiteurs et enregistrent leurs données à des fins de marketing.

Le site web est-il tenu d'informer le visiteur que leurs renseignements personnels sont utilisés à des fins de marketing ?

A) Oui
B) Non

33 / 40
Une entreprise peut se profiler comme un expert dans un domaine particulier d'expertise à l'aide des médias sociaux.

Quel est le **meilleur** moyen de démontrer une expertise dans un domaine particulier ?

A) En affichant des renseignements sur l'entreprise sur les médias sociaux
B) En répondant activement à des questions à propos de ses produits sur les médias sociaux
C) En publiant sur l'infériorité du produit du concurrent
D) En publiant des informations sur les nouveaux produits élaborés par l'entreprise

34 / 40
Une violation de sécurité s'est produite dans un système d'information qui recèle également des données personnelles.

Quelle est la **première** chose que le responsable du traitement doit faire ?

A) Déterminer si la violation peut avoir entraîné la perte ou le traitement illicite de données personnelles
B) Évaluer le risque d'effets indésirables pour les personnes concernées par les données à l'aide d'une analyse d'impact relative à la protection des données (DPIA)
C) Évaluer si un traitement illégal de données personnelles de nature sensible est susceptible d'avoir eu lieu
D) Signaler immédiatement la violation à l'autorité de contrôle pertinente

35 / 40
Le terme "protection des renseignements personnels" n'est pas mentionné dans le Réglement Général de Protection des Données (RGPD) ?

Quel est le lien entre "protection des renseignements personnels" et "protection des données" ?

A) La protection des données est un ensemble de règles et règlementations sur le traitement des données personnelles. La protection des renseignements personnels résulte de la protection des données.
B) La protection des renseignements personnels est le droit à être protégé de l'ingérence dans les affaires personnelles. La protection des données est le moyen de mettre en œuvre cette protection.
C) La protection des renseignements personnels est le droit à garder secrètes les questions personnelles. La protection des données est le droit à préserver le secret des questions personnelles.
D) Les termes "protection des renseignements personnels" et "protection des données" sont interchangeables. Il n'y a pas de réelle différence de sens.

36 / 40
Le règlement (UE) 2016/679, connu sous l'acronyme RGPD, abroge une précédente directive de l'UE.

Quelle est la directive abrogée (remplacée) ?

A) La directive 2002/58/CE du 12 juillet 2002
B) La directive 2006/24/CE du mercredi 15 mars 2006
C) La directive 95/46/CE du mardi 24 octobre 1995
D) La directive 97/66/CE du lundi 15 décembre 1997

37 / 40
Quel droit des personnes concernées par les données est explicitement défini par le Réglement Général de Protection des Données (RGPD) ?

A) Une copie des données personnelles doit être fournie au format demandé par la personne concernée par les données.
B) L'accès gratuit à ses données personnelles pour la personne concernée par les données.
C) Les données personnelles doivent toujours être modifiées à la demande de la personne concernée par ces dernières.
D) Les données personnelles doivent être effacées à tout moment si la personne concernée par ces dernières en fait la demande.

38 / 40
Le Réglement Général de Protection des Données (RGPD) considère les 'données personnelles sensibles' comme une catégorie particulière de données personnelles.

Qu'est-ce qui constitue un exemple de ces données ?

A) Un rendez-vous dans un hôpital avec un spécialiste
B) Un numéro de compte bancaire International (IBAN)
C) Un abonnement à une revue scientifique sur la politique
D) L'adhésion à une association professionnelle

39 / 40
Quel rôle dans la protection des données détermine les finalités et les moyens du traitement de données personnelles ?

A) Responsable du traitement
B) Délégué à la protection des données
C) Sous-traitant

40 / 40

Parmi les informations suivantes, laquelle est considérée par le Réglement Général de Protection des Données (RGPD) comme une donnée personnelle ?

A) Informations relatives une personne, qui pourraient porter atteinte à la vie privée de cette personne, même si elles sont fausses

B) Toute information concernant une personne physique identifiable

C) Toute information concernant une personne physique identifiable et numérisée

Solutions de l’examen

1 / 40
La collecte, le stockage, la modification, la divulgation ou la diffusion illégale de données personnelles est une infraction au droit européen.

De quel type d'infraction s'agit-il ?

A) Une infraction relative au contenu
B) Une infraction d'ordre économique
C) Une infraction à la propriété intellectuelle
D) Une infraction à la protection des renseignements personnels

A) Incorrect. Une infraction relative au contenu se rapporte à la diffusion de propos racistes, de (pédo)pornographie ou d'informations incitant à la violence.
B) Incorrect. Une infraction d'ordre économique se rapporte à un accès non autorisé à des systèmes (piratage, diffusion de virus, etc.), à l'espionnage informatique, les faux en informatique et l'utilisation frauduleuse d'un ordinateur.
C) Incorrect. Les délits relatifs à la propriété intellectuelle se rapportent à des violations du droit d'auteur et des droits connexes.
D) Correct. Tout traitement illégal de donnée personnelle constitue un délit. Source : aucune source : connaissances de base.

2 / 40
Quel est le rapport entre la protection de la vie privée et la protection des données ?

A) La protection des données fait partie de la protection de la vie privée.
B) La protection de la vie privée fait partie de la protection des données.
C) Il s'agit de la même chose.
D) La protection de la vie privée ne peut être réalisée sans protection des données.

A) Incorrect. La protection de la vie privée couvre de nombreux concepts tels que la protection des données géographiques, la protection des relations, la protection corporelle et la protection des informations. La protection des données n'a aucun lien avec certains de ces concepts.
B) Incorrect. La protection de la vie privée couvre de nombreux concepts tels que la protection des données de géolocalisation, la protection des relations, la protection corporelle et la protection des informations. La protection des données contribue à garantir certains de ces objectifs.
C) Incorrect. La protection des données, entre autres, n'a rien à voir avec la protection des données de géolocalisation.
D) Correct. La protection des données est une mesure nécessaire pour protéger le droit fondamental à la vie privée. Source : White Paper – Privacy, Personal Data and the GDPR - §1.3 Definitions

3 / 40
À quoi est **principalement** destiné le Réglement Général de Protection des Données (RGPD) ?

A) À servir de base commune sur laquelle les états membres peuvent élaborer leurs propres lois
B) À faire en sorte que les pays non membres de l'UE respectent le droit à la vie privée des individus au sein de l'UE
C) À garantir la protection des renseignements personnels en tant que droit fondamental de chaque être humain
D) À renforcer et unifier la protection des données des individus au sein de l'UE

A) Incorrect. Le RGPD est une règlementation, ce qui signifie qu'il abroge les lois nationales de protection des données des états membres.
B) Incorrect. Son objectif principal vise à définir les droits en matière de protection des données des individus au sein de l'UE.
C) Incorrect. Le RGPD indique explicitement que la protection des données est un droit fondamental, mais sa portée est limitée aux individus au sein de l'UE.
D) Correct. La portée du RGPD est limitée à la protection des données en tant que droit des individus au sein de l'UE et vise à harmoniser les règles à cet effet au sein de l'UE. Source : EU GDPR, A pocket guide – Introduction.

4 / 40
Le Réglement Général de Protection des Données (RGPD) a trait à la protection des données personnelles.

Quelle est la définition des données personnelles ?

A) Toute information concernant une personne physique identifiée ou identifiable
B) Toute information que les citoyens européens souhaitent protéger
C) Les données qui révèlent, directement ou indirectement, l'origine raciale ou ethnique, les convictions religieuses d'une personne, et les données relatives à sa santé ou à ses habitudes sexuelles
D) Préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information

A) Correct. Telle est la définition officielle de la protection des données. Source : EU GDPR, A pocket guide - Chapter 2 Terms and definitions GDPR 2016/679 Article 4: definition
B) Incorrect. Cette définition est trop générale.
C) Incorrect. C'est la définition des données sensibles et non celle des données personnelles plus générales.
D) Incorrect. C'est la définition de la sécurité de l'information par la norme ISO/IEC 27000:2014.

5 / 40
Selon le Réglement Général de Protection des Données (RGPD), quelle catégorie de données personnelles est considérée comme des données sensibles ?

A) Les informations de carte de crédit
B) L'appartenance à un syndicat
C) Le numéro de passeport
D) Le numéro de sécurité sociale

A) Incorrect. Le RGPD ne considère pas les informations de carte de crédit comme des données sensibles.
B) Correct. L'appartenance à un syndicat constitue une donnée sensible. Source : RGPD art. 9, rec.10 - Catégories spéciales de données personnelles.
C) Incorrect. Le RGPD ne considère pas les informations sur un passeport comme des données sensibles.
D) Incorrect. Le RGPD ne considère pas le numéro de sécurité sociale comme une donnée sensible.

6 / 40
Selon le Réglement Général de Protection des Données (RGPD), quelle est la définition du "traitement" de données personnelles ?

A) Toute opération qui peut être effectuée sur des données personnelles
B) Toute opération qui peut être effectuée sur des données personnelles à l'exception de leur effacement et de leur destruction
C) Uniquement les opérations au cours desquelles les données sont partagées sur les médias sociaux ou transférées par courriel ou par tout autre moyen utilisant Internet
D) Uniquement les opérations dans lesquelles les données personnelles sont utilisées aux fins pour lesquelles elles ont été recueillies

A) Correct. Source : RGPD art. 4 (2)
B) Incorrect. "traitement" signifie toute opération qui est effectuée sur des données personnelles.
C) Incorrect. "traitement" signifie toute opération qui est effectuée sur des données personnelles.
D) Incorrect. "traitement" signifie toute opération qui est effectuée sur des données personnelles.

7 / 40
"Une autorité publique indépendante qui est établie par un état membre conformément à l'article 51."

De quel rôle dans la protection des données est-ce la définition ?

A) Responsable du traitement
B) Sous-traitant
C) Autorité de contrôle
D) Tiers

A) Incorrect. Voir le règlement 2016/679, Article 4.
B) Incorrect. Voir le règlement 2016/679, Article 4.
C) Correct. Source : RGPD 2016/679, Article 4 et Article 51.
D) Incorrect. Voir le règlement 2016/679, Article 4.

8 / 40
En vertu du Réglement Général de Protection des Données (RGPD), un 'consentement éclairé' constitue une base légale du traitement des données personnelles. L'objectif du traitement pour lequel le consentement est donné doit être documenté.

À quel moment dans le processus, le consentement de la personne concernée doit-il être obtenu ?

A) Après que les caractéristiques de la finalité aient été communiquées et avant la collecte des données personnelles
B) Avant que les caractéristiques de la finalité ne soient élaborées et présentées
C) Avant le traitement des données personnelles
D) Avant la publication ou la diffusion des données personnelles

A) Correct. Le consentement peut uniquement être donné en connaissance de cause après que les caractéristiques de la finalité aient été présentées à la personne concernée par les données. Source : RGDP recitals (32), (42).
B) Incorrect. Le consentement peut uniquement être donné en connaissance de cause après que les caractéristiques de la finalité aient été présentées à la personne concernée par les données.
C) Incorrect. La collecte de données personnelles constitue un 'traitement' et doit, en tant que telle, bénéficier du consentement éclairé de la personne concernée par les données.
D) Incorrect. La publication et la diffusion de données personnelles constitue un 'traitement' et doivent, en tant que telles, bénéficier du consentement éclairé de la personne concernée par les données.

9 / 40
Le principe de proportionnalité et de subsidiarité constitue l'une des bases du Réglement Général de Protection des Données (RGPD).

Quel est le sens de la 'proportionnalité' dans ce contexte ?

A) Les données personnelles peuvent uniquement être traitées conformément aux caractéristiques de la finalité.
B) Les données personnelles ne peuvent pas être réutilisées sans un consentement explicite et éclairé.
C) Les données personnelles ne peuvent être traitées que dans le cas où il n'existe pas d'autres moyens d'atteindre les objectifs.
D) Les données personnelles doivent être adéquates, pertinentes et non excessives au regard des finalités.

A) Incorrect. C'est l'une des limitations légales.
B) Incorrect. C'est l'une des limitations légales.
C) Incorrect. C'est la définition de la subsidiarité.
D) Correct. Source : White Paper – Privacy, Personal Data and the GDPR - § 3.1.2 Proportionality and subsidiarity, GDPR art. 35 (7)

10 / 40
Le traitement des données personnelles doit répondre à certains critères de qualité.

Quel est l'un de ces critères de qualité définis par le Réglement Général de Protection des Données (RGPD) ?

A) Les données traitées doivent être archivées.
B) Les données traitées doivent être encodées.
C) Les données traitées doivent être indexées.
D) Les données traitées doivent être pertinentes.

A) Incorrect. Ce critère n'est pas défini par le RGPD.
B) Incorrect. Ce critère n'est pas défini par le RGPD.
C) Incorrect. Ce critère n'est pas défini par le RGPD.
D) Correct. Ce critère est défini par le RGPD. Source : White Paper – Privacy, Personal Data and the GDPR - § 3.1.2 Proportionality and subsidiarity

11 / 40
Chaque fois que des données personnelles sont traitées, il convient de vérifier la proportionnalité et la subsidiarité.

Quelles sont les exigences applicables aux données personnelles traitées ?

A) Elles doivent toujours être limitées au strict nécessaire permettant d'atteindre les objectifs définis et aux données les moins "intrusives".
B) Elles doivent être manipulées par le nombre le plus restreint possible d'employés et ces derniers doivent travailler pour le responsable du traitement ou une filiale.
C) Elles doivent être limitées à une taille de stockage prédéfinie et le système utilisé doit être financé par le responsable du traitement.
D) Elles doivent être utilisées pour le plus petit nombre de buts possible et leur utilisation doit rester confinée aux locaux du sous-traitant.

A) Correct. Ces conditions signifient que vous collectez uniquement les données nécessaires pour atteindre le ou les objectifs prédéfinis, et que vous essayez toujours d'utiliser des données ayant le moins d'impact possible sur la vie privée de la personne concernée. Source : EU GDPR, A pocket guide - Chapter 3 The Regulation – Lawful processing
B) Incorrect. Le nombre d'employés ou leur appartenance à une quelconque filiale n'a aucun rapport avec ces conditions.
C) Incorrect. La taille de stockage et l'origine du financement des systèmes utilisés n'a rien à voir avec ces conditions.
D) Incorrect. Tant que la personne concernée donne son consentement, ni le nombre d'objectifs ni l'emplacement ne sont expressément limités.

12 / 40
"Le responsable du traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées pour veiller à ce que (...) seules soient traitées les données personnelles nécessaires à chaque objectif."

De quel terme du Réglement Général de Protection des Données (RGPD) est-ce la définition ?

A) Conformité
B) Protection des données par défaut
C) Protection des renseignements personnels dès la conception
D) Protection intégrée

A) Incorrect. La conformité est le fait de satisfaire des règles ou des normes.
B) Correct. Par défaut, il convient de traiter un minimum de données personnelles pendant la période la plus brève possible, en utilisant les meilleures mesures de sécurité afin d'empêcher tout accès non autorisé. Source : EU GDPR, A pocket guide - Chapter 3 The Regulation – Data protection by design and by default & GDPR art. 20 (2).
C) Incorrect. Protection des données dès la conception fait référence à une conception incluant les mesures appropriées pour la mise en œuvre des principes de protection des données.
D) Incorrect. La protection des données intégrée est le résultat de la protection des données dès la conception.

13 / 40
Quel est le terme utilisé dans le Réglement Général de Protection des Données (RGPD) pour une divulgation de données personnelles ou un accès non autorisés à ces dernières ?

A) Violation de confidentialité
B) violation de données
C) Incident
D) Incident de sécurité

A) Incorrect. Le RGPD utilise le terme 'vioation de données'. Toutes les violations de données ne constituent pas une violation de confidentialité.
B) Correct. Source : EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches & GDPR article 4 (12)
C) Incorrect. Le RGPD utilise le terme violation de données'. Tous les incidents ne constituent pas une violation de données.
D) Incorrect. Le RGPD utilise le terme 'violation de données'. Tous les incidents de sécurité ne constituent pas une violation de données.

14 / 40
Il a été établi qu'une violation de données personnelles sensibles s'est produite.

D'après le Réglement Général de Protection des Données (RGPD), à qui cela doit être signalé en dernier ressort ?

A) L'autorité de contrôle
B) Le délégué à la protection des données (DPO)
C) Le responsable du service
D) La police

A) Correct. Les violations de données doivent être déclarées à l'Autorité de Contrôle (DPA) dans la mesure où elles sont susceptibles d'avoir un impact significatif sur la sécurité de la personne concernée par les données ou sur la sécurité de ses données personnelles. Source : EU GDPR, A pocket guide - Chapter 3 The Regulation Data breaches & GDPR article 4 (12)
B) Incorrect. Même si elles peuvent être signalées à un délégué à la protection des données interne, en fin de compte elles doivent être signalées à l'Autorité de Contrôle (DPA).
C) Incorrect. Même si elles peuvent être signalées à un manager, en fin de compte elles doivent être signalées à l'Autorité de Contrôle (DPA).
D) Incorrect. Les violations de données ne doivent pas nécessairement être signalées à la police, mais en fin de compte, il faut les signaler à l'Autorité de Contrôle (DPA).

15 / 40
Le disque d'un serveur de données se plante lors d'une sauvegarde. Les données et la sauvegarde sont perdues. Le disque contenait des données personnelles mais pas de données sensibles.

De quel genre d'incident s'agit-il ?

A) Violation de données
B) Violation de sécurité
C) Incident de sécurité

A) Correct. La perte irrémédiable de données personnelles est considérée comme un traitement non autorisé, ce qui en fait une violation de données. Source : EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches & GDPR Chapter I, Article 4, Definitions.
B) Incorrect. La perte irrémédiable de données personnelles est considérée comme un traitement non autorisé, ce qui en fait une violation de données.
C) Incorrect. La perte irrémédiable de données personnelles est considérée comme un traitement non autorisé, ce qui en fait une violation de données.

16 / 40
Une personne travaillant pour un syndicat a emporté chez elle un projet de bulletin d'information à envoyer aux membres pour finir d'y travailler. La clé USB contenant le projet et la liste de diffusion, a été perdu.

À qui, entre autres, cette violation de données devrait-elle être signalée ?

A) Tous les membres sur la liste de diffusion
B) Le personnel du syndicat
C) La police

A) Correct. Il s'agit de données sensibles. La perte doit donc être être signalée à la fois à l'autorité de contrôle et aux personnes concernées par les données. Source : EU GDPR, A pocket guide - Chapter 3 The Regulation – Data breaches
B) Incorrect. Il s'agit de données sensibles, donc la perte doit être signalée à la fois à l'autorité de contrôle et aux personnes concernées par les données.
C) Incorrect. Il s'agit de données sensibles, donc la perte doit être signalée à la fois à l'autorité de contrôle et aux personnes concernées par les données.

17 / 40
Un organisme de services sociaux prévoit de concevoir une nouvelle base de données pour gérer ses clients et les soins dont ils ont besoin.

Quelle est l'une des premières mesures importantes à prendre en vue de demander l'autorisation à l'autorité de contrôle ?

A) Recueillir des données sur les clients ainsi que sur la quantité et le type de soins requis et fournis.
B) Effectuer une analyse d'impact relative à la protection des données (DPIA) pour évaluer les risques du traitement prévu.
C) Obtenir le consentement des clients pour le traitement de leurs données personnelles.

A) Incorrect. La collecte des données personnelles médicales constitue, par définition, un traitement de données sensibles. L'autorisation de l'Autorité de Contrôle (DPA) et de la personne concernée doit être obtenue préalablement.
B) Correct. Lors de la demande de consentement au traitement de données, la personne concernée "devrait être informée des risques, des règles, des garanties et des droits ..." Source : EU GDPR, A pocket guide - Chapter 3 The Regulation – Consent & GDPR recital (39).
C) Incorrect. Lors de la demande de consentement au traitement de données, la personne concernée "devrait être informée des risques, des règles, des mesures de protection et des droits ..." Une PIA est préalablement nécessaire afin d'évaluer ces risques et ces mesures de protection.

18 / 40
Dans quel cas, les personnes concernées devraient-elles toujours être informées d'une violation de données ?

A) Lorsque les données personnelles ont été traitées dans les locaux d'un sous-traitant qui ne sont pas situés à l'intérieur des frontières de l'Union Européenne
B) Lorsque les données personnelles ont été traitées par une partie qui a donné son accord sur un projet de contrat avec le responsable du traitement mais n'a pas encore signé le contrat
C) Lorsque le système sur lequel les données ont été traitées a subi une attaque endommageant ses unittés de stockage
D) Lorsqu'il y a une probabilité significative que la violation ait des conséquences négatives sur la protection de la vie privée des personnes concernées

A) Incorrect. L'emplacement du traitement n'a pas de signification quant à l'obligation de notification de violation aux personnes concernées.
B) Incorrect. Le traitement de données personnelles par une autre partie que le responsable du traitement, sans un contrat écrit valide, est considéré comme une violation de données. Toutefois, dans ce cas précis, les conséquences négatives pour les personnes consernées sont peu probables. La notification des personnes concernées n'est pas obligatoire dans ce cas.
C) Incorrect. Les dommages aux unités de stockage rendront l'accès aux données difficile, voire impossible, mais cela 'nimplique pas un traitement illicite.
D) Correct. S'il y a une probabilité significative d'impact négatif pour les personnes concernées, le responsable du traitement a l'obligation de les informer de la violation des données. Source: White Paper – Privacy, Personal Data and the GDPR - § 5.2 Procédures à suivre en cas de violation de données.

19 / 40
Un responsable de traitement a confié un contrat de traitement de données personnelles sensibles à un sous-traitant dans un pays d'Afrique du Nord, sans consulter l'autorité de contrôle. Une fois découvert, il fut pénalisé par l'autorité de contrôle. Six mois plus tard l'autorité constate que le responsable du traitement se rend coupable de la même faute pour une autre opération de traitement.

Quelle est la peine maximale que l'autorité de contrôle peut imposer dans ce cas ?

A) € 750 000
B) €1 230 000
C) € 10 000 000 ou 2% du chiffre d'affaires mondial annuel de l'entreprise, la pénalité la plus importante étant appliquée
D) € 20 000 000 ou 4% du chiffre d'affaires mondial annuel de l'entreprise avec un minimum de 20 000 000 €, la pénalité la plus importante étant appliquée

A) Incorrect. Selon l'article du RGPD numéro 83.3 L'amende maximale est de 4 % du chiffre d'affaires mondial avec un minimum de € 20 000 000.
B) Incorrect. Selon l'article du RGPD numéro 83.3 L'amende maximale est de 4 % du chiffre d'affaires mondial avec un minimum de € 20 000 000.
C) Incorrect. Selon l'article du RGPD numéro 83.3 L'amende maximale est de 4 % du chiffre d'affaires mondial avec un minimum de € 20 000 000
D) Correct. C'est le maximum pour une infraction. Source : White Paper – Privacy, Personal Data and the GDPR - §7.3.3 General conditions for imposing administrative fines.

20 / 40
Les Autorités de Contrôle assument un certain nombre de responsabilités visant à s'assurer que la réglementation sur la protection des données est respectée.

Qu'est ce qui constitue l'une de ces responsabilités ?

A) L'évaluation des codes de conduite pour des secteurs spécifiques en matière de traitement de données personnelles
B) La définition d'un ensemble minimum de mesures à prendre afin de protéger les données personnelles
C) Enquêter sur toutes les violations de données dont elles ont été averties
D) L'évaluation de la conformité aux réglementations des contrats et des règles d'entreprise contraignantes

A) Correct. L'une des responsabilités des Autorités de Contrôle consiste à fournir des conseils généraux sur la façon de se conformer aux règlementations. Source : White Paper – Privacy, Personal Data and the GDPR - §7.1.4 To set standards.
B) Incorrect. Une Autorité de Contrôle (DPA) vous donnera des conseils généraux sur ce qu'elle considère comme un niveau de sécurité approprié. Elle n'indique toutefois pas les mesures spécifiques à prendre pour atteindre ce niveau. Quand bien même elle le voudrait, elle ne le pourrait pas car il n'y a pas de solution systématique pour toutes les situations.
C) Incorrect. Les Autorités de Contrôle (DPA) n'ont ni l'obligation, ni la capacité d'enquêter sur toutes les violations dont elles ont la connaissance. Toutefois, elles enquêtent sur celles qu'elles jugent significatives ou dignes d'attention.
D) Incorrect. Une Autorité de Contrôle (DPA) n'est pas un conseil juridique. Elles n'examinent pas les contrats ou les règles d'entreprise contraignantes. Cependant, dans le cadre d'une enquête il se peut qu'elles jettent un œil sur un contrat spécifique ou un ensemble de règles d'entreprise contraignantes.

21 / 40
Une association religieuse veut partager des données personnelles avec leur autorité religieuse dans un pays non européen afin de répondre à une demande du gouvernement concerné.

Quelle est la réglementation du Réglement Général de Protection des Données (RGPD) applicable dans ce cas ?

A) À titre exceptionnel, une association religieuse est autorisée à traiter des données sensibles révélant les croyances religieuses.
B) Il est illégal de transférer des données personnelles hors de la zone Économique Européenne en réponse à une exigence légale d'un pays tiers.
C) Le traitement est licite si le consentement spécifique et non équivoque de la personne concernée a été acquis.
D) Le traitement de données personnelles en dehors de la zone économique européenne est autorisé si les clauses du contrat modèle conçu par la Commission de l'UE ont été utilisées.

A) Incorrect. Les associations religieuses sont autorisées à traiter des données personnelles relatives à leurs membres, anciens et actuels, mais elles n'ont pas le droit de transférer des données personnelles hors de l'UE en réponse à une exigence légale d'un pays tiers.
B) Correct. Source : White Paper – Privacy, Personal Data and the GDPR - §7.5.2 Regulations applying to data transfer outside the EEA & EU GDPR, A pocket guide - Chapter 3: The regulation – International transfers & GDPR art. 48.
C) Incorrect. Il est illégal de transférer des données personnelles hors de l'UE en réponse à une exigence légale d'un pays tiers, *même avec le consentement de la personne concernée par les données.*
D) Incorrect. Le traitement des données sensibles à l'extérieur de l'UE peut être légal, mais pas en réponse à une demande du gouvernement d'un pays tiers.

22 / 40
Le 12 juillet 2016, la Commission européenne a mis en œuvre un arrêté concernant le transfert de données personnelles avec les États-Unis (EU-US Privacy Shield).

En termes de Réglement Général de Protection des Données (RGPD), de quel type d'arrêté s'agit-il ?

A) Une décision d'adéquation
B) Un décret d'exception
C) Un contrat contraignant standard
D) Un traité remplaçant le RGPD

A) Correct. L'arrêté est une décision d'adéquation conformément au RGPD et relative au traitement dans des pays tiers. Source : White Paper – Privacy, Personal Data and the GDPR - §7.5.4 Regulations applying to data transfer between the EEA and the USA & EU GDPR, A pocket guide - Chapter 3 The Regulation – International transfers & GDPR recitals 104 and 106.
B) Incorrect. Une exception porte sur les transferts essentiels pour répondre aux infractions terroristes ou en matière de crimes graves (art. 11)
C) Incorrect. L'arrêté est une décision d'adéquation conformément au RGPD et relative au traitement dans des pays tiers.
D) Incorrect. L'arrêté est une décision d'adéquation conformément au RGPD et relative au traitement dans des pays tiers.

23 / 40
Pour les entreprises, les règles d'entreprise contraignantes sont un moyen d'alléger leur fardeau administratif en vue de se conformer au Réglement Général de Protection des Données (RGPD).

De quelle manière ces règles les aident-elles ?

A) Elles leur permettent de disposer de contrats de sous-traitance avec toutes les parties concernées à l'étranger.
B) Elles leur permettent de confier le traitement de données personnelles à des tiers hors zone économique européenne.
C) Elles permettent de ne plus avoir à démarcher séparément chaque autorité de contrôle au sein de l'UE.
D) Elles permettent aux entreprises de ne plus avoir à demander l'autorisation de traiter des données à une autorité de contrôle, une fois que leurs règles contraignantes ont été acceptées.

A) Incorrect. Les règles d'entreprise contraignantes sont rédigées pour permettre aux entreprises de ne plus utiliser de contrat de sous-traitance pour chaque filiale.
B) Incorrect. Les règles d'entreprise contraignantes sont uniquement applicables dans une organisation et l'ensemble de ses filiales. Elles ne s'appliquent pas aux autres parties.
C) Correct. Une fois que les règles d'entreprise contraignantes sont approuvées par une Autorité de Contrôle (DPA) au sein de l'UE, il n'est plus nécessaire de demander aux autres DPA au sein de l'UE de les approuver. Source : EU GDPR, A pocket guide - Chapter 3 The Regulation – Binding corporate rules
D) Incorrect. Les règles d'entreprise contraignantes doivent également être approuvées par une Autorité de Contrôle (DPA).

24 / 40
Si une entreprise externalise le traitement des données personnelles, les parties passent un contrat écrit. Ce contrat décrit l'objet et la durée du traitement, la nature et le but du traitement, le type de données personnelles et les catégories de personnes concernées par les données.

Quel autre aspect doit être régi par ce contrat écrit ?

A) La responsabilité du sous-traitant
B) L'obligation de notification des violations de données
C) L'obligation du sous-traitant de coopérer avec l'autorité de contrôle
D) Les droits et obligations du responsable du traitement

A) Incorrect. C'est une obligation directe imposée aux sous-traitants par le RGPD.
B) Incorrect. C'est une obligation directe imposée aux sous-traitants par le RGPD.
C) Incorrect. C'est une obligation directe imposée aux sous-traitants par le RGPD.
D) Correct. C'est une obligation directe imposée aux sous-traitants par le RGPD. Source : EU GDPR, A pocket guide - Chapter 3 The Regulation – Controller/processor contracts & GDPR art. 28 (3).

25 / 40
Que faut-il entreprendre pour qu'un responsable du traitement soit en mesure d'externaliser le traitement de données personnelles auprès d'un sous-traitant ?

A) Le responsable du traitement doit demander à l'autorité de contrôle l'autorisation d'externaliser le traitement des données.
B) Le responsable du traitement doit demander à l'autorité de contrôle si le contrat écrit convenu est conforme à la réglementation.
C) Le responsable du traitement et le sous-traitant doivent rédiger et signer un contrat écrit garantissant la confidentialité des données.
D) Le sous-traitant doit montrer au responsable du traitement que toutes les exigences convenues dans le contrat de niveau de service (SLA) sont remplies.

A) Incorrect. Il n'est pas nécessaire de demander l'accord de l'Autorité de Contrôle (DPA) pour instance de sous-traitance.
B) Incorrect. L'Autorité de Contrôle (DPA) n'a pas vocation à fournir des conseils juridiques et ne vérifie pas la conformité des contrats.
C) Correct. Un contrat doit être rédigé pour garantir la confidentialité des données et dans lequel le responsable du traitement définit les objectifs et les moyens du traitement. Les deux parties doivent signer ce contrat. Source : EU GDPR, A pocket guide - Chapter 3 The Regulation – Controller/processor contracts & GDPR art. 28 (3).
D) Incorrect. Un SLA n'est pas suffisant car il se concentre sur les activités, pas nécessairement sur la définition d'objectifs.

26 / 40
La protection des données dès la conception, telle que définie à l'article 25 du RGPD est basée sur sept principes clés. L'un d'eux est généralement appelé *'Functionality – Positive-Sum, not Zero-Sum'* .

Quelle est l'essence de ce principe ?

A) Les normes de sécurité appliquées doivent assurer la confidentialité, l'intégrité et la disponibilité des données personnelles tout au long de leur cycle de vie.
B) Si différents types d'objectifs légitimes sont contradictoires, les objectifs visant la protection des renseignements personnels doivent être prioritaires sur les autres objectifs de sécurité.
C) Lors de l'intégration de la protection des renseignements personnels dans une technologie, un processus ou un système donné, cela devrait être fait de manière à ne pas entraver les fonctionnalités.
D) Dans la mesure du possible, il convient de mener une évaluation détaillée de l'impact sur et des risques pour la protection des renseignements personnels, de la publier et de documenter clairement les risques pour la protection des renseignements personnels.

A) Incorrect. Il s'agit d'un aspect de l'un des autres six principes de base, intitulé "End-to-End Security – Lifecycle Protection" (sécurité de bout en bout - protection du cycle de vie)
B) Incorrect. La protection des renseignements personnels dès la conception rejette l'approche selon laquelle la protection des renseignements personnels doit entrer en concurrence avec d'autres intérêts légitimes, les objectifs de la conception et les capacités techniques. Tous les objets doivent être intégrés d'une manière 'à somme positive', "gagnant-gagnant".
C) Correct, voilà son essence. Source : White Paper – Privacy, Personal Data and the GDPR - § 8.1.1 The seven principles of data protection by design & GDPR art 25
D) Incorrect. Il s'agit d'un aspect de la 'protection des renseignements personnels' *intégrée* à la conception', l'un des autres six principes de base

27 / 40
Souvent, le personnel travaillant avec des données personnelles considère leur protection et la sécurité de l'information comme deux sujets distincts.

Pourquoi est-ce une erreur ?

A) La protection des renseignements personnels ne peut être garantie sans l'identification, la mise en œuvre et le suivi de mesures de sécurité adéquates de l'information.
B) L'autorité de contrôle s'attend à ce que les rôles de délégué à la protection des données et de chargé de la sécurité de l'information soient intégrés.
C) Les règlementations identifient des mesures spécifiques de sécurité de l'information qui doivent être prises avant d'autoriser le traitement des données personnelles.

A) Correct. La protection des renseignements personnels et la protection des données visent, notamment, la garantie de la confidentialité des données personnelles. Cela nécessite la mise en œuvre de mesures de sécurité. Source : White Paper – Privacy, Personal Data and the GDPR - § 2.1.6 - integrity and confidentiality.
B) Incorrect. L'Autorité de Contrôle (DPA) ne s'attend pas du tout à ce que ces rôles soient intégrés.
C) Incorrect. Les réglementations précisent les objectifs à atteindre, mais pas de mesures spécifiques à prendre.

28 / 40
L'un des objectifs d'une analyse d'impact relative à la protection des données (DPIA) est de "renforcer la confiance des clients ou des citoyens dans la façon dont les données personnelles sont traitées et la protection des renseignements personnels est respectée".

Comment une DPIA peut-elle "renforcer la confiance" ?

A) L'organisation minimise le risque de coûteux ajustements au sein de processus ou de restructuration de systèmes à un stade ultérieur.
B) L'organisation évite la non-conformité au RGPD et minimise le risque d'amendes.
C) L'organisation démontre qu'elle prend la protection des renseignements personnels au sérieux et qu'elle vise la conformité au RGPD.

A) Incorrect. Cet aspect peut renforcer la confiance de la direction, mais pas celle des clients ou des citoyens.
B) Incorrect. Le fait d'éviter les amendes peut renforcer la confiance de la direction, mais pas celle des clients ou des citoyens.
C) Correct. Source : EU GDPR, A pocket guide - Chapter 3 The Regulation - Data Protection Impact Assessments

29 / 40
Quel est le but d'un audit sur la protection des données par l'autorité de contrôle ?

A) S'acquitter de l'obligation imposée par le Réglement Général de Protection des Données (RGPD) consistant à mettre en œuvre des mesures techniques et organisationnelles appropriées pour la protection des données
B) Assurer l'application du RGPD en vérifiant que le traitement a lieu conformément à ce dernier
C) Conseiller le responsable du traitement quant à l'atténuation des risques sur la protection des renseignements personnels, afin de protéger le responsable du traitement de toute action en responsabilité pour non-conformité au RGPD

A) Incorrect. L'audit ne constitue pas la mise en œuvre des mesures, mais est une évaluation de leur efficacité.
B) Correct. Selon le RGPD, il s'agit d'une tâche importante de l'Autorité de Contrôle (DPA) en tant qu'autorité de contrôle. Source : GDPR art 57.1(a)
C) Incorrect. L'Autorité de Contrôle (DPA) a pour tâche de surveiller la conformité et de fournir des conseils sur les améliorations, mais son objectif n'est pas de protéger le responsable du traitement.

30 / 40
Qu'est-ce qui décrit le **mieux** le principe de minimisation des données ?

A) Il convient de recueillir le moins de données possible afin de protéger les renseignements personnels et les intérêts des personnes concernées par les données.
B) Les données doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.
C) Pour faire en sorte que les données restent gérables, il convient de les stocker de manière à ce qu'elles nécessitent un minimum d'espace de stockage.
D) Le nombre d'éléments collectés pour chaque personne concernée ne doit pas dépasser la limite supérieure stipulée par l'autorité de contrôle.

A) Incorrect. En fait, le RGPD stipule que les données collectées doivent être adéquates, et n'impose en rien un strict minimum.
B) Correct. C'est la définition exacte de la minimisation des données. Son objectif est de s'assurer que seules les données nécessaires pour atteindre les objectifs définis sont recueillies. Source : White Paper – Privacy, Personal Data and the GDPR - §2.1 Data processing principles & GDPR article 5.1.c.
C) Incorrect. La taille du stockage n'a rien à voir avec ce principe.
D) Incorrect. Les Autorités de Contrôle (DPA) ne fixent aucune limite maximale au nombre d'éléments recueillis tant que ces derniers se limitent à ce qui est nécessaire pour atteindre les objectifs visés.

31 / 40
Les cookies de session sont l'un des types de cookies les plus communs.

Qu'est-ce qui décrit le **mieux** un cookie de session ?

A) Il contient des informations sur ce que vous faites, par exemple les produits que vous sélectionnez dans une boutique en ligne, avant de finaliser votre commande.
B) Il révèle l'historique de votre navigation, de sorte que d'autres sites web peuvent identifier les sites web que vous avez visités avant d'arriver là où vous êtes actuellement.
C) Il enregistre l'historique de votre navigation, afin de vous permettre de conserver la trace des sites visités et d'y revenir si vous le souhaitez.
D) Il recueille vos données personnelles, permettant au site web de vous saluer par votre nom et de réutiliser vos paramètres lorsque vous revenez.

A) Correct. Un cookie de session est conservé en mémoire pour enregistrer des informations sur la session. Il est effacé lorsque vous fermez la session. Source : White Paper – Privacy, Personal Data and the GDPR - § 8.6.3 Cookies
B) Incorrect. Un cookie de session est effacé lorsque vous fermez la session. Il ne peut donc pas être utilisé dans une prochaine session.
C) Incorrect. Un cookie de session est effacé lorsque vous fermez la session. Il ne peut donc pas être utilisé dans une prochaine session.
D) Incorrect. Un cookie de session est effacé lorsque vous fermez la session. Il ne peut donc pas être utilisé dans une prochaine session.

32 / 40
Parfois certains sites web suivent les visiteurs et enregistrent leurs données à des fins de marketing.

Le site web est-il tenu d'informer le visiteur que leurs renseignements personnels sont utilisés à des fins de marketing ?

A) Oui
B) Non

A) Correct. Le site web est dans l'obligation d'avertir le visiteur que ses renseignements personnels sont utilisés à des fins de marketing. Le visiteur a le droit de s'opposer au traitement des données personnelles le concernant à des fins de marketing. Source : White Paper – Privacy, Personal Data and the GDPR - § 8.6.3 Cookies
B) Incorrect. Le site web est dans l'obligation d'avertir le visiteur que ses renseignements personnels sont utilisés à des fins de marketing. Le visiteur a le droit de s'opposer au traitement des données personnelles le concernant à des fins de marketing.

33 / 40
Une entreprise peut se profiler comme un expert dans un domaine particulier d'expertise à l'aide des médias sociaux.

Quel est le **meilleur** moyen de démontrer une expertise dans un domaine particulier ?

A) En affichant des renseignements sur l'entreprise sur les médias sociaux
B) En répondant activement à des questions à propos de ses produits sur les médias sociaux
C) En publiant sur l'infériorité du produit du concurrent
D) En publiant des informations sur les nouveaux produits élaborés par l'entreprise

A) Incorrect. Se contenter de publier des informations sur une entreprise n'en fait pas un expert.
B) Correct. Le fait de répondre (activement) sur les médias sociaux à des questions au sujet d'un produit spécifique pourrait faire de votre entreprise un expert. Source : White Paper – Privacy, Personal Data and the GDPR - § 8.6. Practice related applications of the use of data, marketing and social media.
C) Incorrect. Cela revient juste à se vanter des qualités de votre produit (qui n'est peut-être pas si bien que cela).
D) Incorrect. Cela revient juste à montrer que votre entreprise élabore de nouveaux produits. Cela peut contribuer à améliorer les ventes, mais ne fait pas de l'entreprise un expert.

34 / 40
Une violation de sécurité s'est produite dans un système d'information qui recèle également des données personnelles.

Quelle est la **première** chose que le responsable du traitement doit faire ?

A) Déterminer si la violation peut avoir entraîné la perte ou le traitement illicite de données personnelles
B) Évaluer le risque d'effets indésirables pour les personnes concernées par les données à l'aide d'une analyse d'impact relative à la protection des données (DPIA)
C) Évaluer si un traitement illégal de données personnelles de nature sensible est susceptible d'avoir eu lieu
D) Signaler immédiatement la violation à l'autorité de contrôle pertinente

A) Correct. Source : White Paper – Privacy, Personal Data and the GDPR - § 5.2 Procedures on how to act when a data breach occurs.
B) Incorrect. Une PIA est menée lors de la conception des activités de traitement des données personnelles.
C) Incorrect. Le responsable du traitement doit tout d'abord déterminer si l'incident est une violation de données qui doit être signalée.
D) Incorrect. Le responsable du traitement doit tout d'abord déterminer si l'incident est une violation de données qui doit être signalée.

35 / 40
Le terme "protection des renseignements personnels" n'est pas mentionné dans le Réglement Général de Protection des Données (RGPD) ?

Quel est le lien entre "protection des renseignements personnels" et "protection des données" ?

A) La protection des données est un ensemble de règles et règlementations sur le traitement des données personnelles. La protection des renseignements personnels résulte de la protection des données.
B) La protection des renseignements personnels est le droit à être protégé de l'ingérence dans les affaires personnelles. La protection des données est le moyen de mettre en œuvre cette protection.
C) La protection des renseignements personnels est le droit à garder secrètes les questions personnelles. La protection des données est le droit à préserver le secret des questions personnelles.
D) Les termes "protection des renseignements personnels" et "protection des données" sont interchangeables. Il n'y a pas de réelle différence de sens.

A) Incorrect. La protection des renseignements personnels est un droit, la protection des données est le moyen de l'appliquer.
B) Correct. Source : White Paper – Privacy, Personal Data and the GDPR - § 1.3 Definitions.
C) Incorrect. La protection des renseignements personnels est un droit, la protection des données est le moyen de l'appliquer.
D) Incorrect. La protection des renseignements personnels est un droit, la protection des données est le moyen de l'appliquer.

36 / 40
Le règlement (UE) 2016/679, connu sous l'acronyme RGPD, abroge une précédente directive de l'UE.

Quelle est la directive abrogée (remplacée) ?

A) La directive 2002/58/CE du 12 juillet 2002
B) La directive 2006/24/CE du mercredi 15 mars 2006
C) La directive 95/46/CE du mardi 24 octobre 1995
D) La directive 97/66/CE du lundi 15 décembre 1997

A) Incorrect. La directive 2002/58/CE modifie certaines parties de la directive 97/66/CE.
B) Incorrect. Cette directive porte sur la conservation des données recueillies notamment par les fournisseurs d'accès à Internet.
C) Correct. Ce remplacement est mentionné dans le (sous) titre de la réglementation. Source : RGPD.
D) Incorrect. Cette directive complète la directive 95/46/CE afin de garantir un niveau équivalent de protection des droits et libertés fondamentales dans les états membres.

37 / 40
Quel droit des personnes concernées par les données est explicitement défini par le Réglement Général de Protection des Données (RGPD) ?

A) Une copie des données personnelles doit être fournie au format demandé par la personne concernée par les données.
B) L'accès gratuit à ses données personnelles pour la personne concernée par les données.
C) Les données personnelles doivent toujours être modifiées à la demande de la personne concernée par ces dernières.
D) Les données personnelles doivent être effacées à tout moment si la personne concernée par ces dernières en fait la demande.

A) Incorrect. Elle doit être fournie dans un format électronique structuré et couramment utilisé, mais pas nécessairement dans le format demandé par la personne concernée par les données.
B) Correct. Cependant, seule la première copie doit être fournie gratuitement. Source : EU GDPR, A pocket guide – Chapter 3 The Regulation – Data subjects' rights.
C) Incorrect. Seules les données erronées doivent être corrigées.
D) Incorrect. L'article 17 cite quelques exceptions, notamment lorsque les données sont requises pour l'établissement, l'exercice ou la défense d'un droit en justice.

38 / 40
Le Réglement Général de Protection des Données (RGPD) considère les 'données personnelles sensibles' comme une catégorie particulière de données personnelles.

Qu'est-ce qui constitue un exemple de ces données ?

A) Un rendez-vous dans un hôpital avec un spécialiste
B) Un numéro de compte bancaire International (IBAN)
C) Un abonnement à une revue scientifique sur la politique
D) L'adhésion à une association professionnelle

A) Correct. Un rendez-vous avec un spécialiste relève de la catégorie "données personnelles concernant la santé". Voir le RGPD, art. 9.1.
B) Incorrect. Un IBAN se rapporte uniquement à une personne, c'est donc une donnée personnelle. Il ne s'agit toutefois pas de données personnelles sensibles aux termes du RGPD art. 9.
C) Incorrect. Une revue scientifique sur la politique ne relève pas des 'données à caractère personnel révélant les opinions politiques, les croyances religieuses ou philosophiques' et ne fait donc pas partie des données personnelles sensibles aux termes du RGPD art. 9.
D) Incorrect. Seules une affiliation à un syndicat et toute autre donnée personnelle 'révélant (...) les opinions politiques, les croyances religieuses ou philosophiques' sont considérées comme données personnelles sensibles aux termes du RGPD art. 9.

39 / 40
Quel rôle dans la protection des données détermine les finalités et les moyens du traitement de données personnelles ?

A) Responsable du traitement
B) Délégué à la protection des données
C) Sous-traitant

A) Correct. Responsable du traitement : une personne physique ou morale, autorité publique, agence ou tout autre organisme qui, seul ou conjointement, détermine les finalités et les moyens du traitement de données personnelles. Source : White Paper – Privacy, Personal Data and the GDPR - §1.4 Roles, responsibilities, stakeholders.
B) Incorrect.
C) Incorrect.

40 / 40
Parmi les informations suivantes, laquelle est considérée par le Réglement Général de Protection des Données (RGPD) comme une donnée personnelle ?

A) Informations relatives une personne, qui pourraient porter atteinte à la vie privée de cette personne, même si elles sont fausses
B) Toute information concernant une personne physique identifiable
C) Toute information concernant une personne physique identifiable et numérisée

A) Incorrect. Toute déclaration relative à une personne physique identifiable est considérée comme donnée personnelle par le RGPD.
B) Correct. Source : EU GDPR, A pocket guide – Chapter 2 Term and definitions - Personal data & GDPR art.4 (1).
C) Incorrect. Toute déclaration relative à une personne physique identifiable est considérée comme donnée personnelle par le RGPD.

Évaluation

Le tableau ci-dessous indique les bonnes réponses aux questions de cet exemple d'examen.

Question	Réponse	Question	Réponse
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

Contacter EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER