# EXIN Privacy & Data Protection

## ESSENTIALS

Certified by EXIN

Exemple d'examen

Édition 201901

# Table des matières

# Introduction

Voici l'exemple d'examen EXIN Privacy and Data Protection Essentials (PDPE.FR). Les règles et réglementations d'examens EXIN s'appliquent à cet examen.

Cet exemple d'examen consiste en 20 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 20. Chaque réponse correcte rapporte un point. Si vous obtenez 13 points ou plus vous réussissez votre examen.

Le temps alloué lors de l'examen est de 30 minutes.

Bonne chance!

# Exemple d’examen

**1 / 20**
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 / 20**
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 / 20**
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.

**4 / 20**
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 / 20**
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

**6 / 20**
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.

**7 / 20**
*"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 / 20**
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

**9 / 20**
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

**10 / 20**
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 / 20**
*"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

**12 / 20**
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

**13 / 20**
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.

**14 / 20**
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

**15 / 20**
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

**16 / 20**
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.

**17 / 20**
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.

**18 / 20**
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.

**19 / 20**
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.

**20 / 20**
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

# Solutions de l’examen

**1 / 20**
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 / 20**
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 / 20**
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.

**4 / 20**
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 / 20**
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.

**6 / 20**
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.

**7 / 20**
*"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 / 20**
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.

**9 / 20**
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.

**10 / 20**
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 / 20**
*"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.

**12 / 20**
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.

**13 / 20**
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.

**14 / 20**
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.

**15 / 20**
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.

**16 / 20**
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).

**17 / 20**
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.

**18 / 20**
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.

**19 / 20**
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.

**20 / 20**
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.

# Évaluation

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

| Question | Réponse | Question | Réponse |
|---|---|---|---|
| 1 | D | 11 | B |
| 2 | D | 12 | B |
| 3 | B | 13 | B |
| 4 | A | 14 | D |
| 5 | B | 15 | A |
| 6 | B | 16 | C |
| 7 | C | 17 | C |
| 8 | A | 18 | A |
| 9 | A | 19 | A |
| 10 | D | 20 | A |

# Contacter EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER