Nom : _____ Date : _____ Note : _____

Protéger les données personnelles et Vos droits

Données personnelles, droits à la vie privée (RGPD (GDPR), CCPA), courtiers en données, cookies, hameçonnage, VPN et comptes plus sûrs

PRÉSENTATION DE L'APPRENTISSAGE : CONFIDENTIALITÉ DES DONNÉES PERSONNELLES

ÉCLAIRÉ

CONNAÎTRE VOS DONNÉES

Ce qui est collecté et pourquoi

RENFORCÉ

DROITS À LA VIE PRIVÉE

Droits RGPD (GDPR) et CCPA/CPRA

VIGILANT

BONNES HABITUDES

MFA, mises à jour et détection des arnaques

Bienvenue ! Ce dossier d'activités vous aide à reprendre le contrôle de vos données personnelles. Vous étudierez les droits en matière de vie privée prévus par le RGPD (GDPR) et le CCPA, les courtiers en données, le consentement aux cookies, les autorisations des applications, l'hameçonnage, le Wi-Fi public, les VPN et l'authentification multifacteur (MFA).

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : découvrez vos droits en matière de vie privée et les bonnes pratiques.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

Ouvrir le guide VPN.com de la confidentialité des données

URL: https://www.vpn.com/fr/cybersecurite/confidentialite-donnees/

Votre parcours d'apprentissage : confidentialité des données personnelles

- Comprendre vos droits en matière de vie privée selon le RGPD (GDPR) et le CCPA californien.
- Identifier comment les courtiers en données, les cookies et les applications collectent des données personnelles.
- Appliquez la minimisation des données en ne partageant que ce dont un service a réellement besoin.
- Faire des choix éclairés face aux bandeaux de cookies et aux demandes d'autorisation des applications.
- Réduisez le risque lié à l'hameçonnage, aux fuites de données et aux Wi-Fi publics grâce à la MFA et aux mises à jour.

INSTRUCTIONS DU GUIDE SUR LA PROTECTION DES DONNÉES PERSONNELLES

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances à la protection de vos propres données personnelles. Terminez par l'activité bonus Réflexion rapide.

CONFIDENTIALITÉ DES DONNÉES PERSONNELLES ET VOS DROITS (INTRODUCTION)

La confidentialité des données est votre capacité à contrôler la manière dont vos informations personnelles sont collectées, utilisées, stockées et partagées. Des lois comme le RGPD (GDPR) et le CCPA vous donnent des droits, tandis que de bonnes habitudes comme des mots de passe robustes, l'authentification multifacteur (MFA) et un partage prudent peuvent aider à réduire les risques.

LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.

Point de contrôle 1 : Défi QCM

1. Quel choix reflète le mieux le principe de minimisation des données ?

- A. Ne partager que les données dont un service a besoin pour sa finalité
- B. Donner à chaque application un accès complet pour faciliter la configuration
- C. Remplir tous les champs facultatifs des formulaires d'inscription
- D. Réutiliser un même mot de passe pour gérer plus facilement ses comptes

2. Quelle mesure est recommandée si un site que vous utilisez signale une fuite de données ?

- A. Changer ce mot de passe et activer la MFA lorsqu'elle est proposée
- B. Réutiliser le même mot de passe pour un nouveau compte
- C. Répondre à l'e-mail signalant la fuite en indiquant votre code PIN
- D. L'ignorer, car les fuites de données ont rarement de l'importance

3. Selon les règles européennes, qu'est-ce qui constitue un consentement valable aux cookies de pistage ?

- A. Cocher activement une case non cochée après une information claire
- B. Cases précochées sur une bannière de cookies ou d'inscription
- C. Simplement continuer à faire défiler ou à parcourir le site web
- D. Un avis caché dans les conditions générales du site

4. De quel droit les consommateurs californiens disposent-ils en vertu du CCPA ?

- A. S'opposer à la vente ou au partage de leurs données
- B. Être payé un montant fixe pour chaque demande de données
- C. Pour exiger le retrait de n'importe quelle application des boutiques d'applications
- D. Pour bloquer toute collecte de données par toutes les entreprises

5. Que fait principalement un VPN lorsque vous vous connectez à un Wi-Fi public ?

- A. Chiffre le trafic entre votre appareil et le serveur VPN
- B. Empêche les sites web de déposer le moindre cookie
- C. Remplace le besoin de MFA
- D. Supprime les logiciels malveillants déjà présents sur un appareil

Point de contrôle 2 : Défi Vrai ou Faux

6 Question vrai/faux 6

6. La confidentialité des données et la sécurité des données signifient la même chose.

○ Vrai ○ Faux

7 Question vrai/faux 7

7. Le RGPD (GDPR) peut s'appliquer à des entreprises hors UE qui proposent des services à des personnes situées dans l'UE.

○ Vrai ○ Faux

8 Question vrai/faux 8

8. Utiliser un VPN empêche les sites web de vous suivre à l'aide de cookies.

○ Vrai ○ Faux

9 Question vrai/faux 9

9. Partager moins de données personnelles en ligne peut réduire les dommages causés par une fuite de données.

○ Vrai ○ Faux

10 Question vrai/faux 10

10. Le CCPA permet aux consommateurs de refuser la vente ou le partage de leurs données.

○ Vrai ○ Faux

Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Selon le RGPD (GDPR), le _____ doit être libre, spécifique, éclairé et univoque : les cases précochées ne comptent donc pas.

2. Un _____ compile des informations issues de registres publics, d'applications et d'achats pour constituer et vendre des profils de personnes.

3. Un SMS affirmant que votre colis est bloqué et vous demandant de 'confirmer' vos coordonnées bancaires est une tentative typique d' _____ .

4. Le HTTPS utilise le _____ pour aider à protéger les données en transit entre votre navigateur et un site web.

5. Ne communiquer que les informations réellement nécessaires à un formulaire d'inscription applique le principe de _____ .

6. Le droit à l' _____ vous permet de demander à une organisation de supprimer vos données personnelles, même si des exceptions s'appliquent.

BANQUE DE MOTS DE VOCABULAIRE

CHIFFREMENT CONSENTEMENT COOKIE COURTIER EN DONNÉES EFFACEMENT
HAMEÇONNAGE MINIMISATION DES DONNÉES OPT-OUT

Écrivez vos réponses ici :

1. **2.**

3. **4.**

5. **6.**

Point de contrôle 4 : Association de notions sur la vie privée

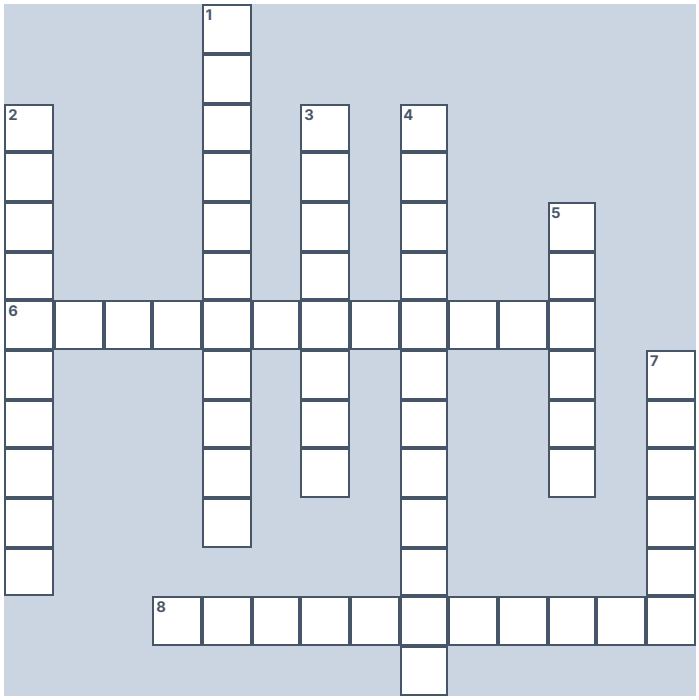
ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

☐	1. Droit à l'effacement	A	Droit californien d'empêcher une entreprise de vendre ou de partager vos données.
☐	2. Droit d'opposition (opt-out)	B	Droit, prévu par le RGPD (GDPR), de faire effacer vos données personnelles, sous réserve d'exceptions.
☐	3. Minimisation des données	C	Petit fichier de navigateur utilisé pour suivre votre activité d'un site web à l'autre.
☐	4. Chiffrement	D	Accord libre, spécifique, éclairé et univoque.
☐	5. Courtier en données	E	Ne collecter que les données personnelles nécessaires à une finalité déclarée.
☐	6. Consentement	F	Faux messages qui incitent les gens à révéler des données ou leurs identifiants de connexion.
☐	7. Hameçonnage (phishing)	G	Brouiller des données pour que seule une personne disposant de la bonne clé puisse les lire.
☐	8. Cookie de suivi	H	Entreprise qui compile et vend des profils personnels issus de nombreuses sources.

Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.



HORIZONTALEMENT

6. Accord libre, spécifique, éclairé et univoque à l'utilisation des données (12)

8. Faux messages qui vous incitent à révéler vos identifiants ou vos coordonnées bancaires (11)

VERTICALEMENT

1. Brouillage des données pour que seule une personne disposant de la bonne clé puisse les lire (11)

2. Droit qui vous permet de demander à une organisation de supprimer vos données personnelles (10)

3. ___ en données : entreprise qui compile et vend des profils de personnes (8)

4. ___ des données : ne collecter que ce qui est nécessaire à une finalité déclarée (12)

5. Droit prévu par le CCPA de faire cesser la vente ou le partage de vos données (mot composé) (6)

7. Petit fichier du navigateur qui peut suivre votre activité d'un site web à l'autre (6)

Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

HORIZONTALEMENT

6 horizontal: Accord libre, spécifique, éclairé et univoque à l'utilisation des données (12 lettres):

8 horizontal: Faux messages qui vous incitent à révéler vos identifiants ou vos coordonnées bancaires (11 lettres):

VERTICALEMENT

1 vertical: Brouillage des données pour que seule une personne disposant de la bonne clé puisse les lire (11 lettres):

2 vertical: Droit qui vous permet de demander à une organisation de supprimer vos données personnelles (10 lettres):

3 vertical: ___ en données : entreprise qui compile et vend des profils de personnes (8 lettres):

4 vertical: ___ des données : ne collecter que ce qui est nécessaire à une finalité déclarée (12 lettres):

5 vertical: Droit prévu par le CCPA de faire cesser la vente ou le partage de vos données (mot composé) (6 lettres):

7 vertical: Petit fichier du navigateur qui peut suivre votre activité d'un site web à l'autre (6 lettres):

Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

T D F H I D R Q M E I R Z S F
N Q V F R E I T R U O C A A Q
E T U O T P O O C O O K I E N
M P T X Q K R U S D N Y B F S
E G A N N O C E M A H X W C J
T A R Z Y Y L G I M R J M H L
N T O H Q Q H Z A O V G U I B
E Y R Y B H L Z G J O P N F W
S C M Z Y G Y O W U K V P F B
N N V T M G V D Y U K R B R X
O M I N I M I S A T I O N E Z
C Y M R Q X I P D A D J Q M V
W W E F F A C E M E N T L E J
H T H G B E I K T S V R Z N E
H E S C A L Q C Z M K V R T U

LISTE DE MOTS DE VOCABULAIRE

EFFACEMENT OPTOUT MINIMISATION CHIFFREMENT COURTIER
CONSENTEMENT HAMECONNAGE COOKIE

Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

TERMES DE VOCABULAIRE

- **A. EFFACEMENT**
- **B. OPTOUT**
- **C. MINIMISATION**
- **D. CHIFFREMENT**
- **E. COURTIER**
- **F. CONSENTEMENT**
- **G. HAMECONNAGE**
- **H. COOKIE**

DÉFINITIONS ET CHAMPS D'ASSOCIATION

1. Droit prévu par le CCPA de faire cesser la vente ou le partage de vos données (mot composé).
2. Accord libre, spécifique, éclairé et univoque à l'utilisation des données.
3. ___ en données : entreprise qui compile et vend des profils de personnes.
4. Droit qui vous permet de demander à une organisation de supprimer vos données personnelles.
5. ___ des données : ne collecter que ce qui est nécessaire à une finalité déclarée.
6. Faux messages qui vous incitent à révéler vos identifiants ou vos coordonnées bancaires.
7. Petit fichier du navigateur qui peut suivre votre activité d'un site web à l'autre.
8. Brouillage des données pour que seule une personne disposant de la bonne clé puisse les lire.

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés de la cybersécurité. Écrivez vos réponses dans les champs prévus.

1. NMECFEETAF
2. NIMIMIONATSI
3. ROCTIREU
4. NGEOMCANHAE
5. OTTOUP
6. FTRMNECHEIF
7. EMECOTTENNNS
8. OECIKO

Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

1	Mesures à prendre après une violation de données			
2	Applications qui demandent votre localisation			
3	Paramètres de confidentialité à vérifier sur un nouveau téléphone			
4	Signes qu'un ordinateur est infecté			
5	Signes qu'un message peut être de l'hameçonnage			
6	Raisons de mettre à jour les logiciels			
7	Informations personnelles à ne pas publier sur les réseaux sociaux			
8	Façons de protéger vos comptes			
9	Informations que vous ne devriez jamais partager			
10	Comptes pour lesquels la MFA devrait être activée			
11	Choses que vous sauvegardez			
12	Endroits où vous pourriez utiliser un Wi-Fi public			
13	Choses à faire après une fuite de données			
14	Entreprises susceptibles de collecter vos données de navigation			
15	Signaux d'alerte dans un e-mail			

Point de contrôle 8 : Études de cas sur la protection des données

Appliquez les notions apprises aux scénarios réels ci-dessous.

ÉTUDE DE CAS 1 : DEMANDER À UN SITE DE SUPPRIMER DES DONNÉES

👨‍💻

Scénario : Maya, qui vit en France, a fermé son compte sur une application d'achat il y a deux ans, mais reçoit toujours ses e-mails marketing. Elle veut que l'application supprime ses données personnelles en vertu du droit à l'effacement prévu par le RGPD (GDPR).

Question de discussion : Quelles démarches Maya pourrait-elle entreprendre, et quelles données l'application pourrait-elle légalement conserver ?

ÉTUDE DE CAS 2 : UNE APPLICATION DE QUIZ ET SES AUTORISATIONS

👨‍💻

Scénario : Une application gratuite de quiz de personnalité demande à Leo sa localisation, ses contacts, l'accès au microphone et sa date de naissance avant qu'il puisse commencer.

Question de discussion : Quelles autorisations semblent inutiles, et de quelles options Leo dispose-t-il pour limiter ce qu'il partage ?

Point de contrôle 9 : Déchiffrer le code

Les personnes soucieuses de leur vie privée prennent le temps de réfléchir avant de partager des informations personnelles en ligne. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les espaces vides.

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

18	5	6	12	5	3	8	9	19	19	5	26		1	22	1	14	20		4	5
		16	1	18	20	1	7	5	18		5	14		12	9	7	14	5		

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

Point de contrôle 10 : Questions fréquentes de base sur la protection des données (Partie A)

Passez en revue les questions et réponses courantes sur la protection de vos données personnelles.

Q1: Quelle est la différence entre confidentialité des données et sécurité des données ?

La confidentialité, c'est le contrôle que vous exercez sur la façon dont vos données personnelles sont collectées, utilisées et partagées ; la sécurité, c'est la protection qui les met à l'abri des accès non autorisés.

Q2: Qu'est-ce que le RGPD (GDPR) ?

Le Règlement général sur la protection des données de l'UE, applicable depuis le 25 mai 2018, fixe des règles pour le traitement des données personnelles et donne aux personnes des droits sur celles-ci [1].

Q3: Qu'est-ce que le CCPA ?

Le California Consumer Privacy Act (CCPA), modifié par le CPRA, donne aux résidents le droit de savoir, de supprimer, de rectifier et de refuser la vente ou le partage de leurs données [4].

Q4: Que signifie la minimisation des données ?

N'utiliser que des données personnelles adéquates, pertinentes et limitées à ce qui est nécessaire pour une finalité ; en tant qu'utilisateur, vous pouvez l'appliquer en partageant moins [1].

Q5: Que sont les autorisations des applications ?

Paramètres qui permettent aux applications d'accéder à votre localisation, à vos contacts ou à vos photos ; les vérifier et désactiver ceux qui sont inutiles peut limiter la collecte de données [8].

Point de contrôle 10 : Questions fréquentes de base sur la protection des données (Partie B)

Passez en revue les questions et réponses courantes sur la protection de vos données personnelles.

Q6: Qu'apporte le HTTPS à ma vie privée ?

HTTPS chiffre les données entre votre navigateur et un site, mais les sites frauduleux peuvent aussi utiliser HTTPS : le cadenas ne prouve donc pas qu'un site est digne de confiance [10].

Q7: Qu'est-ce que le droit à l'effacement ?

En vertu de l'article 17 du RGPD (GDPR), vous pouvez demander à une organisation de supprimer vos données dans certains cas ; ce droit n'est pas absolu et comporte des exceptions [1].

Q8: Qu'est-ce qui constitue un consentement valable ?

Un acte positif clair, comme cocher une case non cochée après une information claire ; les cases précochées, le silence ou le défilement ne comptent pas [2].

Q9: Qu'est-ce qui fait un mot de passe robuste ?

La longueur compte avant tout : le NIST demande aux sites d'exiger au moins 15 caractères pour les mots de passe utilisés seuls et d'autoriser les gestionnaires de mots de passe [11].

Q10: Que faire après une violation de données ?

Changez les mots de passe concernés, activez la MFA, surveillez vos comptes et envisagez un gel gratuit de votre crédit ; IdentityTheft.gov liste les étapes de rétablissement [9].

Point de contrôle 10 : Questions fréquentes avancées sur la vie privée (Partie C)

Approfondissez les questions sur les bases juridiques, les cookies, le pistage, les courtiers en données et vos droits en ligne.

Q1: Tout traitement de données nécessite-t-il mon consentement selon le RGPD (GDPR) ?

Non. Le consentement est l'une des six bases légales de l'article 6 ; les autres incluent le contrat, l'obligation légale et l'intérêt légitime [1].

Q2: Où le RGPD (GDPR) s'applique-t-il ?

Aux organisations établies dans l'UE, ainsi qu'à celles hors UE qui proposent des biens ou des services à des personnes situées dans l'UE ou qui suivent leur comportement [1].

Q3: Les sites web ont-ils besoin d'un consentement pour tous les cookies ?

Pas toujours. Les cookies strictement nécessaires en sont généralement exemptés, mais les cookies non essentiels, comme les cookies de suivi, exigent un consentement préalable valable [3].

Q4: Quel est le risque pour la vie privée des traqueurs tiers ?

Les traqueurs tiers peuvent vous suivre sur de nombreux sites web pour afficher des publicités ciblées ; supprimer les cookies et ajuster les paramètres de confidentialité peut aider [8].

Q5: Qu'est-ce qu'un courtier en données ?

Une entreprise qui collecte des informations personnelles auprès de diverses sources et les revend à d'autres entreprises ; les résidents de Californie peuvent utiliser la plateforme DROP de l'État pour en demander la suppression [5].

Point de contrôle 10 : Questions fréquentes avancées sur la vie privée (Partie D)

Approfondissez les questions sur les bases juridiques, les cookies, le pistage, les courtiers en données et vos droits en ligne.

Q6: Qu'est-ce que le lien CCPA 'Do Not Sell or Share' (Ne pas vendre ni partager) ?

Les entreprises qui vendent ou partagent des données doivent en général proposer un lien « Do Not Sell or Share My Personal Information » et respecter les signaux de refus comme GPC [4].

Q7: Un VPN me rend-il anonyme ?

Non. Un VPN chiffre le trafic jusqu'au serveur VPN et masque votre IP aux sites, mais le fournisseur peut la voir, et les cookies et l'empreinte numérique peuvent toujours vous pister [12].

Q8: Comment repérer un message d'hameçonnage ?

Méfiez-vous des demandes urgentes vous invitant à cliquer sur des liens, à confirmer des informations de paiement ou à régler des problèmes de compte ; contactez l'entreprise via un numéro ou un site web dont vous savez qu'il est authentique [7].

Q9: Le Wi-Fi public est-il sûr ?

Cela peut être risqué. La plupart des sites utilisent le chiffrement : vérifiez donc la présence de HTTPS, maintenez vos logiciels à jour et utilisez la MFA [10] ; un VPN peut ajouter une protection sur les réseaux non fiables [12].

Q10: Quelles sont les sanctions financières maximales prévues par le RGPD (GDPR) ?

Pour les violations les plus graves, les amendes peuvent atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu [1].

Partie 11 : 10 faits et enseignements concrets sur la confidentialité des données

Découvrez des faits concrets sur les lois relatives à la vie privée, les courtiers en données, la fraude, les fuites de données et des habitudes en ligne plus sûres.

1. APERÇU CONFIDENTIALITÉ

Le RGPD (GDPR) s'applique depuis le 25 mai 2018 et donne aux personnes le droit d'accéder à leurs données personnelles, de les rectifier et de les effacer [1].

2. APERÇU CONFIDENTIALITÉ

En vertu du RGPD (GDPR), les violations les plus graves peuvent entraîner des amendes allant jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial [1].

3. APERÇU CONFIDENTIALITÉ

Les modifications apportées par le CPRA au CCPA californien sont entrées en vigueur le 1 janvier 2023 ; elles ajoutent le droit de rectifier les données et de limiter l'usage des données sensibles [4].

4. APERÇU CONFIDENTIALITÉ

Selon la FTC, les consommateurs ont déclaré avoir perdu $15.9 milliards à cause de la fraude en 2025, contre plus de $12 milliards l'année précédente [6].

5. APERÇU CONFIDENTIALITÉ

Depuis le 1er janvier 2026, les résidents de Californie peuvent utiliser la plateforme gratuite DROP pour demander aux courtiers en données de supprimer leurs données personnelles [5].

6. APERÇU CONFIDENTIALITÉ

Selon les règles européennes de protection des données, les cases précochées, le silence ou l'inactivité ne valent pas consentement valable [2].

7. ZOOM SUR LA CONFIDENTIALITÉ

Au Royaume-Uni, les sites doivent vous permettre de consentir à tout cookie qui n'est pas strictement nécessaire au fonctionnement du site [3].

8. ZOOM SUR LA CONFIDENTIALITÉ

Le RGPD (GDPR) exige que certaines violations de données personnelles soient notifiées à l'autorité dans les 72 heures, lorsque cela est possible [1].

9. ZOOM SUR LA CONFIDENTIALITÉ

Selon le NIST, les sites ne devraient pas imposer de changements périodiques de mot de passe et devraient comparer les nouveaux mots de passe à des listes de mots de passe compromis [11].

10. APERÇU CONFIDENTIALITÉ

Un VPN cache votre adresse IP aux sites web, mais le fournisseur du VPN peut toujours voir votre trafic : choisissez-le donc avec soin [12].

Références techniques et sources

Le guide d'étude et les énigmes s'appuient sur les recommandations officielles de l'UE, du Royaume-Uni, de la Californie, de la FTC, du NIST et de l'EFF en matière de vie privée.

RÉFÉRENCES OFFICIELLES ET D'EXPERTS

[1] European Parliament & Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L 119.

https://eur-lex.europa.eu/eli/reg/2016/679/oj

[2] European Data Protection Board. (2020). Guidelines 05/2020 on consent under Regulation 2016/679.

https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[3] Information Commissioner's Office. (n.d.). Cookies. ICO for the public.

https://ico.org.uk/for-the-public/online/cookies/

[4] California Privacy Protection Agency. (n.d.). Frequently asked questions (FAQs).

https://cppa.ca.gov/faq.html

[5] California Privacy Protection Agency. (2025). Delete Request and Opt-out Platform (DROP).

https://privacy.ca.gov/drop/

[6] Federal Trade Commission. (2026, March 25). FTC testifies before the Joint Economic Committee on agency's efforts to combat fraud [Press release].

https://www.ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud

[7] Federal Trade Commission. (2022). How to recognize and avoid phishing scams. Consumer Advice.

https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[8] Federal Trade Commission. (2023). How websites and apps collect and use your information. Consumer Advice.

https://consumer.ftc.gov/articles/how-websites-and-apps-collect-and-use-your-information

[9] Federal Trade Commission. (2024). What to know about identity theft. Consumer Advice.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[10] Federal Trade Commission. (2023). Are public Wi-Fi networks safe? What you need to know. Consumer Advice.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[11] National Institute of Standards and Technology. (2025). Digital identity guidelines: Authentication and authenticator management (NIST SP 800-63B-4).

https://csrc.nist.gov/pubs/sp/800/63/b/4/final

[12] Electronic Frontier Foundation. (2026). Choosing the VPN that's right for you. Surveillance Self-Defense.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

Corrigé : Point de contrôle 1 – Choix multiple

1 **Minimisation des données** MINIMISATION — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

L'article 5 du RGPD (GDPR) exige que les données personnelles soient adéquates, pertinentes et limitées à ce qui est nécessaire ; les utilisateurs peuvent s'en inspirer en partageant moins [1].

2 **Réagir à une violation de données** VIOLATION DE DONNÉES — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Après une violation de données, changez les mots de passe exposés, activez la MFA et surveillez vos comptes ; IdentityTheft.gov propose des étapes de récupération adaptées [9].

3 **Consentement valable** CONSENTEMENT AUX COOKIES — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Un consentement valable exige un acte positif clair après une information claire ; les cases précochées et la poursuite du défilement ne suffisent pas [2].

4 **Droits au titre du CCPA** LOI CCPA — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Les consommateurs californiens peuvent refuser la vente ou le partage de leurs informations personnelles, y compris au moyen des signaux Global Privacy Control [4].

5 **Protection VPN** TUNNEL VPN — **Bonne réponse : A**

NOTE PÉDAGOGIQUE

Un VPN chiffre le trafic jusqu'au serveur VPN et cache votre adresse IP aux sites, mais les cookies et l'empreinte numérique (fingerprinting) peuvent toujours vous suivre [12].

Corrigé : Point de contrôle 2 – Vrai ou faux

6 **Confidentialité ou sécurité** CONFIDENTIALITÉ — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Liés mais différents : l'article 5 du RGPD (GDPR) fixe des règles sur l'utilisation des données, tandis que l'article 32 exige séparément des mesures de sécurité [1].

7 **Champ d'application territorial du RGPD (GDPR)** CHAMP D'APPLICATION DU RGPD — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

L'article 3(2) couvre les organisations hors UE qui proposent des biens ou des services aux personnes se trouvant dans l'UE, ou qui suivent leur comportement [1].

8 **Les VPN et les cookies** LIMITES DES VPN — **Bonne réponse : Faux**

NOTE PÉDAGOGIQUE

Un VPN cache votre adresse IP, mais les cookies, les pixels de suivi et l'empreinte numérique (fingerprinting) peuvent toujours vous suivre d'un site web à l'autre [12].

9 **Partager moins** MINIMISATION — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Désactiver les autorisations d'applications inutiles et partager moins limite ce qui peut être collecté puis exposé lors d'une fuite de données [8].

10 **Refus de la vente ou du partage** LOI CCPA — **Bonne réponse : Vrai**

NOTE PÉDAGOGIQUE

Les entreprises qui vendent ou partagent des données doivent proposer un lien de refus clair, comme « Do Not Sell or Share My Personal Information » [4].

Corrigés du vocabulaire et grille d'évaluation

Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (6 points au total).

POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

B – 1. Droit à l'effacement	A – 2. Droit d'opposition (opt-out)	E – 3. Minimisation des données	G – 4. Chiffrement
H – 5. Courtier en données	D – 6. Consentement	F – 7. Hameçonnage (phishing)	C – 8. Cookie de suivi

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 – CONSENTEMENT	2 – COURTIER EN DONNÉES	3 – HAMEÇONNAGE	4 – CHIFFREMENT
5 – MINIMISATION DES DONNÉES	6 – EFFACEMENT		

POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

1 – B – OPTOUT	2 – F – CONSENTEMENT	3 – E – COURTIER	4 – A – EFFACEMENT
5 – C – MINIMISATION	6 – G – HAMECONNAGE	7 – H – COOKIE	8 – D – CHIFFREMENT

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer Droit à l'effacement, Droit d'opposition (opt-out) et Minimisation des données avec leurs propres mots et donner un exemple pour chacun.

Études de cas :
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

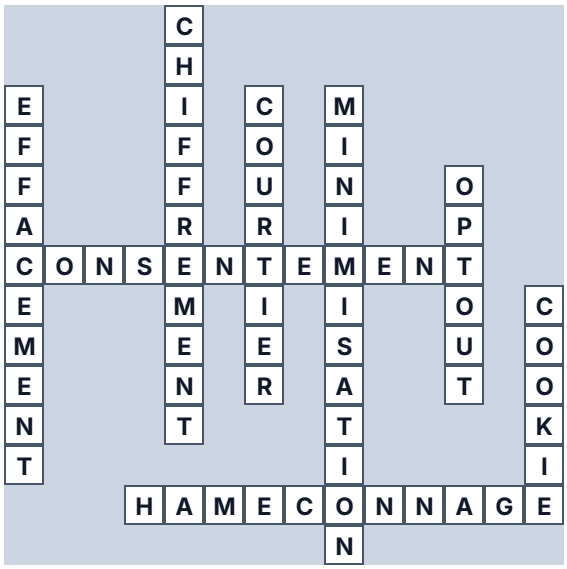
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

T	D	F	H	I	D	R	Q	M	E	I	R	Z	S	F
N	Q	V	F	R	E	I	T	R	U	O	C	A	A	Q
E	T	U	O	T	P	O	O	C	O	O	K	I	E	N
M	P	T	X	Q	K	R	U	S	D	N	Y	B	F	S
E	G	A	N	N	O	C	E	M	A	H	X	W	C	J
T	A	R	Z	Y	Y	L	G	I	M	R	J	M	H	L
N	T	O	H	Q	Q	H	Z	A	O	V	G	U	I	B
E	Y	R	Y	B	H	L	Z	G	J	O	P	N	F	W
S	C	M	Z	Y	G	Y	O	W	U	K	V	P	F	B
N	N	V	T	M	G	V	D	Y	U	K	R	B	R	X
O	M	I	N	I	M	I	S	A	T	I	O	N	E	Z
C	Y	M	R	Q	X	I	P	D	A	D	J	Q	M	V
W	W	E	F	F	A	C	E	M	E	N	T	L	E	J
H	T	H	G	B	E	I	K	T	S	V	R	Z	N	E
H	E	S	C	A	L	Q	C	Z	M	K	V	R	T	U

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

6 horizontal: CONSENTEMENT Accord libre, spécifique, éclairé et univoque à l'utilisation des données (12 lettres)

8 horizontal: HAMECONNAGE Faux messages qui vous incitent à révéler vos identifiants ou vos coordonnées bancaires (11 lettres)

VERTICALEMENT

1 vertical: CHIFFREMENT Brouillage des données pour que seule une personne disposant de la bonne clé puisse les lire (11 lettres)

2 vertical: EFFACEMENT Droit qui vous permet de demander à une organisation de supprimer vos données personnelles (10 lettres)

3 vertical: COURTIER ___ en données : entreprise qui compile et vend des profils de personnes (8 lettres)

4 vertical: MINIMISATION ___ des données : ne collecter que ce qui est nécessaire à une finalité déclarée (12 lettres)

5 vertical: OPTOUT Droit prévu par le CCPA de faire cesser la vente ou le partage de vos données (mot composé) (6 lettres)

7 vertical: COOKIE Petit fichier du navigateur qui peut suivre votre activité d'un site web à l'autre (6 lettres)

Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

CORRIGÉ DES MOTS MÉLANGÉS

1. NMECFEETAF — **EFFACEMENT**
2. NIMIMIONATSI — **MINIMISATION**
3. ROCTIREU — **COURTIER**
4. NGEOMCANHAE — **HAMECONNAGE**
5. OTTOUP — **OPTOUT**
6. FTRMNECHEIF — **CHIFFREMENT**
7. EMECOTTENNNS — **CONSENTEMENT**
8. OECIKO — **COOKIE**

CORRIGÉ DU DÉFI DU CODE SECRET

"REFLECHISSEZ AVANT DE PARTAGER EN LIGNE"

Corrigé des études de cas

A Étude de cas 1 : Demander à un site de supprimer des données

Conseils pour l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : Maya, qui vit en France, a fermé son compte sur une application d'achat il y a deux ans, mais reçoit toujours ses e-mails marketing. Elle veut que l'application supprime ses données personnelles en vertu du droit à l'effacement prévu par le RGPD (GDPR).
- Approches recommandées : Option 1 : Maya envoie une demande d'effacement écrite et s'oppose à la prospection directe, qui doit alors cesser ; l'application doit en général répondre dans un délai d'un mois [1]. Option 2 : elle se désabonne d'abord pour un soulagement rapide. Justification : l'effacement n'est pas absolu, donc l'application peut conserver les données nécessaires au respect d'obligations légales ou à des actions en justice [1]. Si elle ne répond pas, Maya peut porter plainte auprès de son autorité de protection des données [1].

B Étude de cas 2 : Une application de quiz et ses autorisations

Conseils pour l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : une application gratuite de quiz de personnalité demande à Leo sa localisation, ses contacts, l'accès au microphone et sa date de naissance avant qu'il puisse commencer.
- Approches recommandées : Option 1 : refuser l'accès à la localisation, aux contacts et au microphone, puis vérifier si le quiz fonctionne toujours [8]. Option 2 : si l'application insiste, choisir une autre application ou la supprimer [8]. Justification : un quiz a rarement besoin de ces données, et partager moins limite ce qui peut être collecté, vendu ou exposé. Leo peut aussi vérifier régulièrement les autorisations dans les paramètres de confidentialité de son téléphone [8].