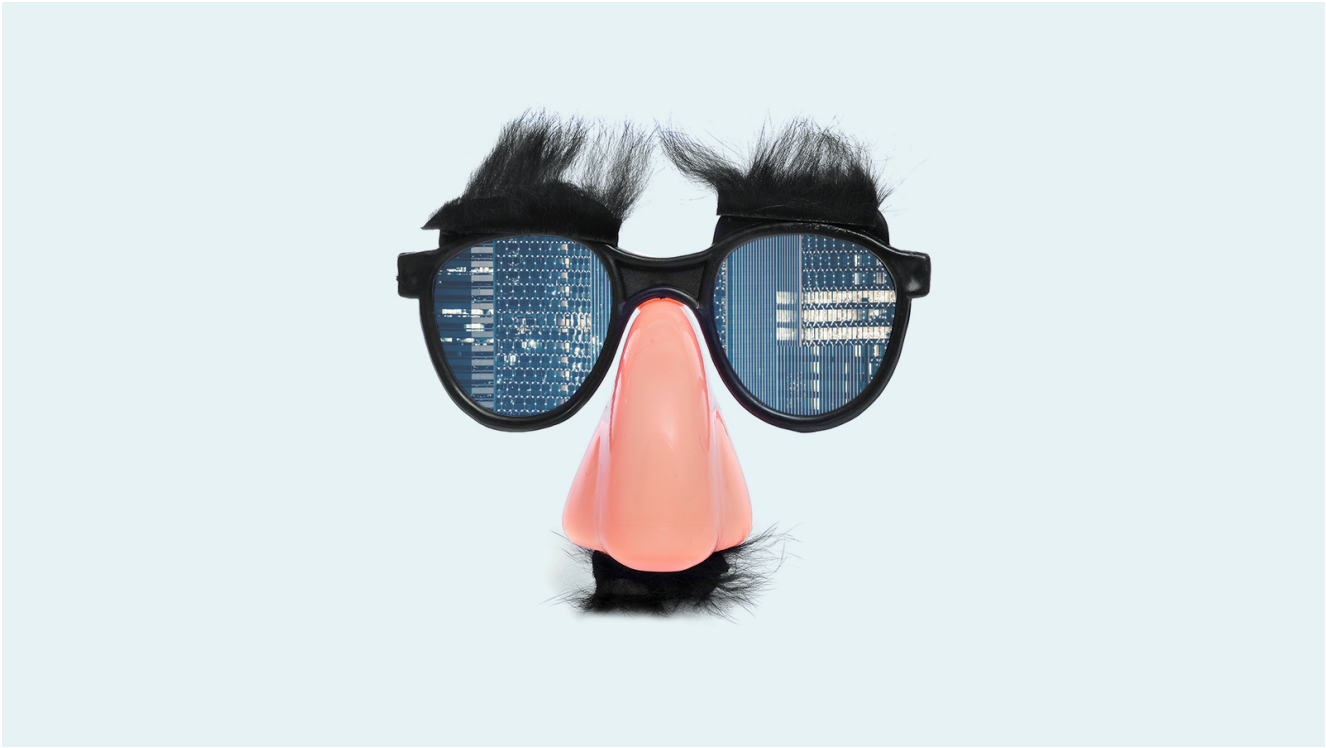
Comprendre la confidentialité des données et son importance

Par Dashlane, gestionnaire de mots de passe que j'utilise depuis quelques années (MC)

W. Perry Wortman :



La confidentialité des données a été un sujet fréquemment abordé ces dernières années. En effet, le partage de données sur le Web, les violations de données, et les règlements gouvernementaux convergent pour mettre en évidence l'importance de la confidentialité des informations et du consentement éclairé.
Alors qu'est-ce que la confidentialité des données et pourquoi est-elle importante ?

Voulez-vous en savoir plus sur l'utilisation du gestionnaire de mots de passe Dashlane pour particulier ou pour entreprise ?

Découvrez nos forfaits pour gestionnaires de mots de passe pour particulier ou commencez avec un essai gratuit pour les entreprises.

Qu'est-ce que la confidentialité des données ?

La **confidentialité des données** désigne notre capacité à contrôler le contenu, le lieu et la manière dont nos informations personnelles ou confidentielles sont collectées, stockées ou partagées.
Bien avant l'ère numérique, la confidentialité des données revêtait une grande importance, mais le Web et les dossiers électroniques ont modifié la signification de ce concept et suscité un intérêt accru pour :

La confidentialité des activités en ligne

Les fournisseurs de services Internet suivent continuellement votre activité en ligne et votre adresse IP, même lorsque vous utilisez des modes de navigation privée ou incognito.
Les lois et règlements sur la confidentialité numérique déterminent la façon dont les informations recueillies lors de la navigation peuvent être utilisées ou pas, et comment nous sommes informés de ce processus.

De nouveaux fournisseurs de moteurs de recherche comme Neeva répondent à la demande du public en offrant des services de navigation privée et sans publicité.
Les membres du forfait Dashlane Premium obtiennent un an d'accès gratuit à Neeva Unlimited, qui offre des outils de confidentialité de qualité et d'autres avantages exclusifs.

Les entreprises protègent nos données personnelles

Dans un contexte de croissance de l'informatique en nuage, du commerce électronique, de la télémédecine et d'autres services en ligne, l'importance des pratiques en matière de protection des données personnelles est mise en évidence dans le but de protéger notre identité et nos informations privées contre les cybercriminels et d'empêcher que les données des consommateurs ne soient utilisées de manière contraire à l'éthique.

- **La confidentialité des données personnelles**

Les données personnelles comprennent des éléments comme votre nom, votre adresse, votre numéro de téléphone et votre numéro de sécurité sociale qui peuvent être utilisés pour vous identifier. Contrairement aux préférences en ligne ou à l'historique de navigation, les données personnelles sont également pertinentes en dehors du monde numérique.
Les données financières, les dossiers médicaux et les dossiers des employés comptent parmi les nombreuses catégories de données personnelles qui doivent être protégées.

- **Les politiques de confidentialité des entreprises**

La confidentialité et la protection des données sont importantes pour les entreprises de bien des façons.
Il est essentiel de préserver la confidentialité des informations de l'entreprise (propriété intellectuelle), des données des employés et des informations partagées avec les clients. Une politique de confidentialité des données définit les règles de base pour le suivi, le stockage et le partage des données des clients collectées sur le site Web de l'entreprise. Cette politique aide également les entreprises à établir une conformité avec une liste croissante de lois relatives à la confidentialité.

Dashlane se consacre à la création de logiciels qui vous aident à contrôler vos informations en ligne.
La Politique de confidentialité de Dashlane comprend des résumés simples en plusieurs langues qui facilitent la compréhension de nos pratiques de collecte, d'utilisation et de partage de données.

Pourquoi la confidentialité des données est-elle importante ?

La confidentialité des données vous aide à contrôler les informations que vous choisissez de garder personnelles.
Tout le monde a le droit d'empêcher que ses données personnelles ne soient utilisées ou partagées sans son consentement, même si ce partage ne conduirait pas à un vol de données ou à d'autres cybercrimes.
La confidentialité des données aide également les entreprises et les particuliers à :

- **Se conformer aux lois relatives à la confidentialité**

En raison de l'importance de la confidentialité des données, une longue liste de lois gouvernementales, fédérales et internationales ont été établies pour protéger notre vie privée en ligne et ailleurs.
Les lois et règlements importants sur la confidentialité et la sécurité des données comprennent :

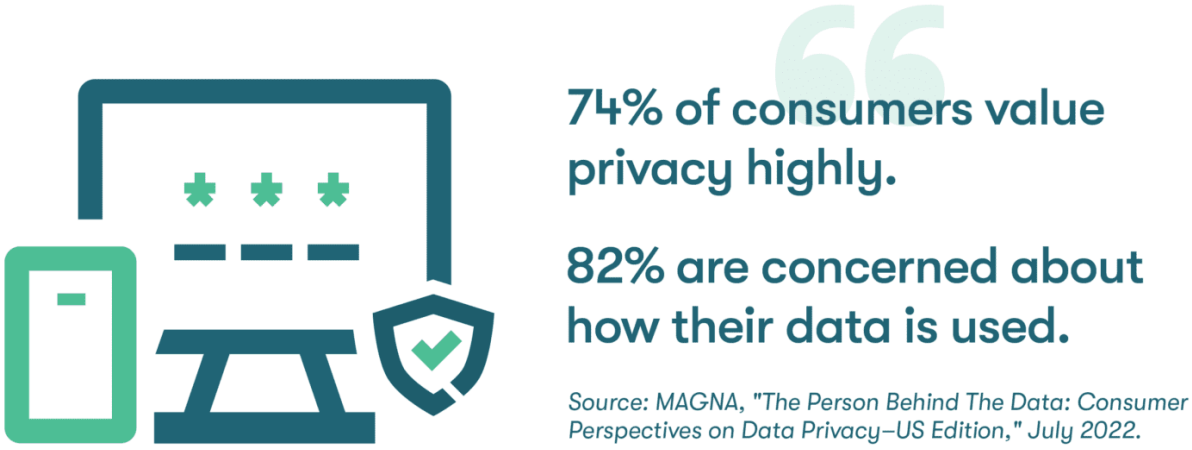
- Children's Online Privacy Protection Act (COPPA) : alors de plus en plus d'enfants utilisent Internet, cette loi fédérale américaine a été établie pour s'assurer que consentement des parents soit obtenu avant toute collecte d'informations personnelles auprès d'enfants de moins de 13 ans.
- Health Insurance Portability and Accountability Act(HIPAA) : cette loi fédérale protège la confidentialité des données de santé collectées par les médecins, les hôpitaux, les compagnies d'assurance ou les employeurs.
- Règlement général sur la protection des données (RGPD) : ce règlement européen établit des normes pour la collecte et l'utilisation des données personnelles en Europe. Cela inclut notamment des droits individuels permettant de refuser la collecte d'informations ou de demander la suppression d'informations.
- California Consumer Privacy Act (CCPA) : établie en 2018, cette loi de l'État de Californie permet aux consommateurs d'avoir davantage de contrôle sur leurs données personnelles que les entreprises peuvent collecter, y compris le droit de savoir quelles données sont collectées et le droit de refuser la vente ou le partage de leurs données personnelles.
- **Prévenir l'usurpation d'identité**

L'usurpation d'identité est l'un des cybercrimes les plus graves liés à la confidentialité et la sécurité des données personnelles.
Il suffit à un usurpateur d'identité de disposer de quelques informations personnellement identifiables (IPI), comme votre nom, votre numéro de permis de conduire et votre numéro de sécurité sociale pour commencer à souscrire à des crédits en votre nom, à voler votre remboursement d'impôt ou à vider votre compte bancaire.

Puisque de nombreuses victimes d'usurpation d'identité ne se rendent compte de ce qui s'est passé qu'une fois le mal fait, la surveillance du dark Web est une pratique recommandée pour analyser en profondeur le Web à la recherche de vos données personnelles et vous informer si des éléments sensibles sont trouvés.

- **Protéger les consommateurs**

La protection des consommateurs est la force motrice de nombreuses lois relatives à la confidentialité.
Il s'agit également d'un facteur important pour les entreprises qui établissent leurs politiques, car selon une étude récente, 74 % des consommateurs accordent une grande importance à la protection de la vie privée tandis que 82 % sont préoccupés par la manière dont leurs données sont collectées et utilisées.
L'impact évident sur la valeur de la marque incite de plus en plus d'entreprises à adopter des politiques transparentes et éthiques en matière de confidentialité des données.



- **Réduire l'impact du piratage et des violations de données**

Alors qu'un piratage est une attaque intentionnelle utilisée pour obtenir un accès non autorisé, une faille de données est le résultat potentiel de cette attaque.
Les pirates informatiques s'efforcent généralement de voler des données confidentielles, telles que les mots de passe, les numéros de carte bancaire, et les informations bancaires, ou d'obtenir des informations confidentielles d'entreprises, comme la propriété intellectuelle, les dossiers financiers et les données des clients.
Dans les deux cas, des pratiques robustes en matière de confidentialité et de sécurité des données peuvent être une dissuasion efficace.

En tant que garant de la protection des données de ses clients, Dashlane est tout à fait conscient de l'importance d'une stratégie rigoureuse en matière de confidentialité des données.
En savoir plus sur notre posture de confidentialité et la façon dont nous l'appliquons dans A Conversation About Privacy: Dashlane "Five Laws."

Les 3 types de protection de données

La confidentialité et la sécurité des données sont étroitement liées à d'autres concepts comme la gestion et la souveraineté des données.
Le concept global de la protection des données rassemble 3 éléments importants :

1. **La protection traditionnelle des données**

La protection traditionnelle des données englobe les pratiques de base du réseau informatique qui existent depuis des décennies.
Cela comprend les plans d'archivage et de conservation des données qui sont également pertinents pour les documents papier.
La protection traditionnelle des données comprend également les pratiques de sauvegarde de réseau, la réplication des données et le RAID et le codage d'effacement pour créer des options de stockage de données plus flexibles.

2. **La sécurité des données**

L'élément sécurité des données de la protection des données comprend les outils utilisés pour protéger la confidentialité des données face aux accès non autorisés, au vol ou à la corruption.
La sécurité des données comprend également les méthodes de sécurité physique utilisées pour protéger les zones où les données confidentielles sont stockées et les méthodes d'authentification qui garantissent que seules les personnes reconnues peuvent afficher ou déplacer des fichiers.
Les outils de cybersécurité supplémentaires utilisés pour améliorer la sécurité des données comprennent :

- Le chiffrement pour brouiller les données dans un format non reconnaissable, ce qui les rend moins vulnérables au piratage et aux failles de données.
- Les gestionnaires de mots de passe pour s'assurer que les comptes privés sont protégés par des mots de passe forts, uniques et stockés en toute sécurité, difficiles à déchiffrer par des pirates informatiques.
- Le VPN pour masquer l'adresse IP et chiffrer toutes les données qui entrent ou sortent d'un appareil tout en les acheminant via un réseau sécurisé.

3. **La confidentialité des données**

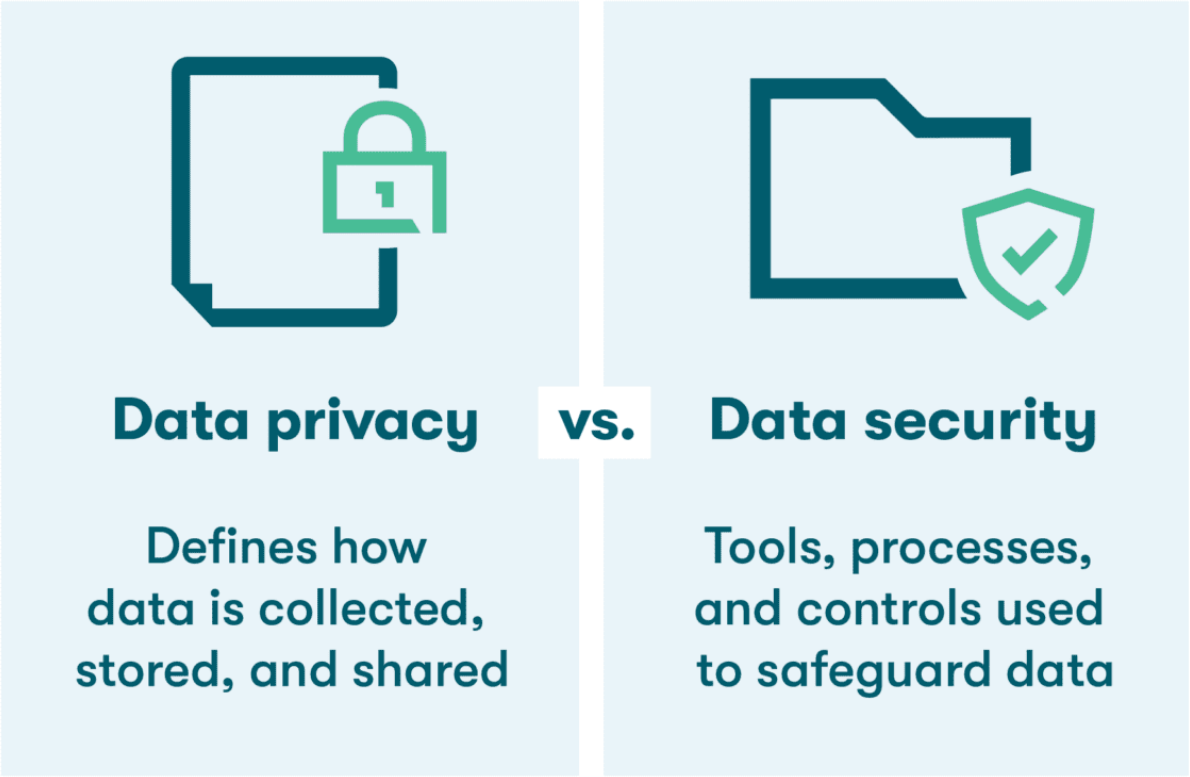
La confidentialité des données est bien plus qu'une collection de logiciels et d'outils utilisés pour garantir la protection des données en ligne.
La confidentialité des données désigne le traitement approprié de toute donnée sensible, y compris les données personnelles, les données financières et la propriété intellectuelle. Les lois, les politiques et les bonnes pratiques conçues pour protéger la confidentialité des données sont basées sur le moment et la façon dont les données personnelles peuvent être collectées et partagées.

Confidentialité des données et sécurité des données : savoir faire la différence

Quel rapport existe-t-il entre la confidentialité des données et la sécurité des données ? Bien qu'il ne s'agisse pas de la même chose, elles jouent chacune un rôle important dans le maintien de la confidentialité des informations et le respect des lois.

- **Les différences**

La **confidentialité des données** définit les lignes directrices pour la gestion et la collecte des données en fonction de leur type et de leur importance, alors que la **sécurité des données** concerne les outils, processus et contrôles de cybersécurité utilisés pour protéger les données.
Les outils de sécurité des données comprennent : les pare-feu, le chiffrement des données, les systèmes de contrôle d'accès et les logiciels de surveillance du réseau.
La sécurité des données assure la protection des données contre les cybermenaces, tandis que la confidentialité des données définit l'utilisation éthique et responsable de celles-ci.



- **Pourquoi la sécurité est-elle nécessaire pour préserver la confidentialité des données ?**

La confidentialité des données et la sécurité des données sont les deux faces d'une même pièce.
Par exemple, si votre organisation recueille des informations personnelles auprès d'acheteurs en ligne pour compléter leurs commandes, votre politique de confidentialité comprendra des stratégies pour le stockage des données à court et à long terme, le partage d'informations avec des tiers et le consentement du client à fournir ses informations.
Une fois que vous avez établi ces règles de base, vous devez vous assurer que vous avez mis en place des outils et des pratiques de sécurité des données adéquats pour protéger les données des clients contre les menaces internes et externes.

- **La protection des données s'applique aux deux**

La protection des données est le terme générique qui recouvre à la fois la confidentialité et la sécurité des données.
La définition initiale de la protection des données, enracinée dans les méthodes traditionnelles, était axée sur le maintien de la disponibilité des données par le biais du processus de sauvegarde du réseau.
Avec la montée en puissance de l'Internet, des services bancaires en ligne et du commerce électronique, la notion de protection des données s'est élargie pour inclure la conservation, la confidentialité et la sécurité des données.
Les activités de préservation des données sont axées sur le maintien de l'intégrité physique ou électronique des fichiers stockés.

Dashlane accorde la priorité à la confidentialité des données

Dashlane permet de générer des mots de passe intuitifs et sécurisés, de les saisir automatiquement sans effort, de les stocker et de les partager dans des coffres-forts sécurisés.
Nous chiffrons et protégeons toutes vos données et métadonnées de façon sécurisée, pas seulement vos mots de passe.
Si Dashlane venait à être compromis (ce qui n'est jamais arrivé), vos informations resteraient protégées.
D'autres outils comme l'analyse des mots de passe, la double authentification (2FA) et la surveillance du dark Web offrent un niveau de sécurité accru.

Notre architecture brevetée « zero-knowledge » garantit que personne, même pas Dashlane, n'a accès à vos données personnelles.
Conformément à la politique de confidentialité de Dashlane, nous ne vous demanderons jamais vos identifiants ni ne stockerons votre mot de passe Maître, et vous pourrez toujours décider de la manière dont les cookies et autres informations sont utilisés.

La confidentialité des données vise à traiter ses données sensibles de façon responsable pour assurer votre sécurité et celle des personnes qui vous entourent. Découvrez comment travailler en toute sécurité en séparant vos données personnelles de celles de votre entreprise dans Notre guide sur la confidentialité des données.

Références

1. Dashlane, « How Safe Is Incognito Mode/Private Browsing, Really? », février 2020.
2. Dashlane, « Dashlane et Neeva s'associent pour sécuriser davantage la recherche en ligne » novembre 2022.
3. ZDNet, « How to create a privacy policy that protects your company and your customers », août 2020.
4. Epic.org, « Children's Privacy », 2023.
5. PrivacyPolicies, « Health Insurance Portability and Accountability Act (HIPAA) », juillet 2022.
6. Investopedia, « General Data Protection Regulation (GDPR) Definition and Meaning » novembre 2020.
7. État de Californie, « California Consumer Privacy Act (CCPA) », février 2023.
8. My Banktracker, « How Much Information is Needed for Someone to Steal Your Identity? », février 2023.
9. Dashlane « Percer l'obscurité du dark Web », juin 2022.
10. Ketch, « The Person Behind The Data », 2023.
11. Dashlane, « Faille de données ou piratage ? Comment les distinguer. », juin 2021.
12. Dashlane, « A Conversation About Privacy: Dashlane's Five Laws », novembre 2021.
13. Qumulo, « Erasure Coding vs. RAID Explained: Methods for Data Protection », décembre 2021.
14. Dashlane, « How to Conduct a Security Audit in Five Steps, », 2023.
15. Dashlane, « Double authentification (2FA) dans Dashlane », 2023.
16. Thales, « A Brief History of Encryption (and Cryptography) », novembre 2022.
17. Scalefusion, « 5 Types of Data Security Tools Every Company Needs in 2023 », août 2022.
18. Dashlane, « La sécurité avant tout : comment Dashlane protège vos données », janvier 2023.
19. Dashlane, « A Deep Dive into Dashlane's Zero-Knowledge Security », juin 2022.
20. Dashlane, « Politique de confidentialité de Dashlane », 2023.
21. Dashlane, « Notre guide sur la confidentialité des données », 2023.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240123
"C'est ensemble qu'on avance"