Confidentialité des données:
Un guide pour les individus et les familles

Protégez vos informations en ligne et préservez votre empreinte numérique.

panda

Table des matières

01.
Notions de base de la confidentialité des données

À l'ère numérique, la confidentialité des données est devenue un véritable sujet d'inquiétude. Un danger qui se cache derrière chaque e-mail envoyé, chaque transaction effectuée et chaque site visité. Pourtant, pour beaucoup, il s'agit aussi d'un concept étranger, souvent négligé jusqu'à ce qu'il soit trop tard.

La confidentialité des données permet de garder vos informations personnelles en sécurité. Les entreprises, les gouvernements et les cybercriminels recherchent tous ces informations pour des raisons diverses, et il est donc essentiel de comprendre comment maintenir la protection de ses données. Heureusement, ce livre électronique complet sur la confidentialité des données donne les informations dont vous avez besoin pour prendre le contrôle de votre empreinte numérique.

Qu'est-ce que la confidentialité des données?

La confidentialité des données est le contrôle qu'un individu ou une organisation exerce sur les informations sensibles stockées ou collectées qui le concernent. Il s'agit de la possibilité de déterminer qui a accès à ces données, comment ces données sont utilisées, et les garanties mises en place pour protéger ces données de toute exposition non autorisée unauthorized exposure.

Les données personnelles en question incluent des informations sensibles telles que noms, adresses, numéros de sécurité sociale ou données financières. Elles s'étendent aussi à des données moins ouvertement personnelles comme les historiques de navigation, données de localisation, adresses IP et contenus de paniers d'achats. Elles peuvent aussi inclure des données biométriques, des dossiers de santé et des renseignements professionnels.

Le concept de confidentialité des données a émergé aux premiers jours de l'informatique, dès lors que des informations personnelles ont été stockées électroniquement pour des raisons diverses. À mesure que le paysage numérique s'est étendu, les utilisations abusives ou les violations de données sont rapidement devenues un sujet de préoccupation.

L'évolution des médias sociaux a en outre accru ces préoccupations. Avec des utilisateurs partageant librement des informations personnelles sur des plateformes telles que Facebook et Twitter, la quantité de données générées a atteint des niveaux sans précédent.

Pourquoi la confidentialité des données est importante

Avec l'évolution exceptionnelle de la technologie, la confidentialité et la protection des données ne sont plus un sujet mineur — elles sont une obligation. La confidentialité des données a pour but de permettre aux individus de contrôler leur empreinte numérique.

Chaque fois que nous nous connectons à Internet, nous générons une quantité importante de données. Des simples likes de médias sociaux à nos habitudes d'achat, ces données en apparence inoffensives dépeignent en fait notre personnalité.

Lorsque ces données privées parviennent dans de mauvaises mains, les répercussions peuvent inclure:

Usurpation d'identité

Le vol de données personnelles peut conduire à des usurpations d'identité. Des personnes peuvent alors se retrouver confrontées à des transactions non autorisées ou des activités criminelles effectuées en leur nom.

Fraude financière

L'accès à des informations financières sensibles peut permettre aux cybercriminels d'effectuer des transactions frauduleuses, avec des pertes financières importantes à la clé.

Perte de confiance

Les entreprises peuvent perdre la confiance de leurs clients et voir ainsi leurs activités se réduire.

Répercussions légales

Les entreprises ne respectant pas les lois et réglementations sur la confidentialité des données peuvent se voir infliger de lourdes amendes et faire l'objet d'actions en justice, avec un impact sur leur réputation et leurs finances.

Augmentation de la cybercriminalité

Le risque de cyberattaques peut augmenter dans la mesure où des données sensibles deviennent facilement accessibles à des pirates.

Perte de confidentialité

Sans confidentialité, nos vies personnelles peuvent être comme un livre ouvert à tous.

Manipulation et exploitation

Les données peuvent être utilisées pour changer des comportements et influencer des décisions, souvent sans le consentement de l'individu et sans même qu'il en soit conscient.

Protection des données vs. Confidentialité des données vs. Sécurité des données

Protection des données, confidentialité des données et sécurité des données sont trois concepts liés mais distincts dans l'univers des données numériques.

En résumé, la protection des données, la confidentialité des données et la sécurité des données se complètent. Chacune a un rôle distinct, mais ensemble, elles créent un environnement numérique sûr.

02.
Informations personnelles et informations personnelles sensibles

Dans le vaste paysage de la confidentialité des données, comprendre la différence entre informations personnelles et informations personnelles sensibles est vital pour respecter la législation, gérer correctement les risques et respecter des considérations éthiques. Une telle compréhension éclaire sur les pratiques de traitement des données, guide les mesures de sécurité et aide à minimiser les dommages potentiels pour les individus au cas où les données seraient compromises.

Cette section présente les différents niveaux de classification des données et explique comment protéger les détails les plus intimes de votre identité numérique.

Qu'est-ce qu'une information personnelle?

Les informations personnelles, souvent appelées données personnelles, sont toutes les informations qui peuvent être utilisées pour identifier une personne spécifique. Elles englobent un large éventail de données pouvant être liées à une personne en particulier. Selon le contexte, elles peuvent inclure des noms, des adresses, des numéros de téléphone, etc.

Comment contrôler vos informations personnelles

To effectively control your personal information, it's essential to adopt proactive measures that enhance your online privacy and security. Let's look at some important tips to keep in mind.

Limitez l'exposition aux médias sociaux

Passez en revue et réglez vos paramètres de confidentialité sur les plateformes de médias sociaux afin de contrôler qui peut voir vos publications et vos informations personnelles.

Réfléchissez avant de publier

Avant de partager des informations personnelles en ligne, réfléchissez aux conséquences potentielles et à la nécessité réelle de divulguer ces informations.

Lisez les politiques de confidentialité

Prenez le temps de lire et de comprendre les politiques de confidentialité des sites Web et des applications que vous utilisez pour savoir comment vos données sont collectées, stockées et partagées.

Refusez la collecte de données

Refusez la collecte de données chaque fois que c'est possible et choisissez des services qui ne vous demandent que des informations essentielles
only ask for essential information.

Qu'est-ce qu'une information personnelle sensible?

Les informations personnelles sensibles sont une catégorie d'informations personnelles considérées comme plus critiques et nécessitant des niveaux de protection plus élevés. Elles comprennent des détails qui, s'ils sont révélés, peuvent avoir des conséquences graves telles que l'usurpation d'identité, le cyberharcèlement ou la discrimination.

Comment contrôler vos informations personnelles sensibles

De nos jours, le contrôle de vos informations personnelles sensibles est plus crucial que jamais. Avec l'augmentation des violations de données et autres cybermenaces, il est essentiel de prendre des mesures proactives pour protéger ces données précieuses.

Soumettre un formulaire de demande d'accès aux données personnelles (DADP)

- **Connaissez vos droits:** En vertu du règlement général sur la protection des données (RGPD), vous avez le droit de demander à une organisation si elle traite ou non vos données.
- **Accédez aux informations:** Une demande d'accès de personne concernée (DADP) vous permet d'accéder aux informations stockées à votre sujet et de comprendre leur utilisation.
- **Demandez une rectification:** Demandez la rectification des données incorrectes ou leur suppression. Les entreprises sont tenues de s'y conformer dans un délai d'un mois civil pour le RGPD et de 45 jours pour la loi californienne California Privacy Rights Act (CPRA).

Utiliser les liens "Ne pas vendre ou partager mes informations personnelles"

- **Consultez les sites Web des entreprises:** Recherchez des options avancées telles que "Ne pas vendre ou partager mes informations" en vertu du California Privacy Rights Act (CPRA) sur les pages d'accueil et les pages de politique de confidentialité des sites Web des entreprises.
- **Refusez:** Refusez que vos informations personnelles ou sensibles soient vendues ou partagées avec des tiers ; les entreprises sont légalement tenues de s'y conformer.

Refuser la collecte sur les sites Web ou dans les navigateurs

- **Effectuez une recherche en ligne:** Effectuez une recherche en ligne sur votre nom pour trouver des sites Web de courtiers de données tels que Radaris, Pipl, Spokeo et Whitepages répertoriant vos informations.
- **Demandez la suppression des données:** Accédez aux pages de retrait de ces plateformes ou envoyez un e-mail pour demander la suppression de vos données.
- **Utilisez des ressources:** Utilisez des ressources telles que le Privacy Rights Clearinghouse pour obtenir un répertoire complet des sites Web et de leurs options de retrait.
- **Lisez les politiques de protection de la vie privée:** Consultez les politiques de confidentialité de vos institutions financières pour refuser le partage des données avec les courtiers.

03.
Violations de données

Vous avez probablement entendu parler d'entreprises ayant subi des violations massives de données et vous vous êtes demandé « Comment cela a-t-il pu se produire ? » ou « Et si j'avais été touché ? ». Une violation de données peut être choquante, mais elle peut aussi avoir des conséquences graves comme des fraudes à la carte bancaire ou même des usurpations d'identité

Voici un examen plus approfondi de la manière dont les violations de données peuvent vous affecter, de la façon dont elles se produisent et de comment les prévenir.

Qu'est-ce qu'une violation de données?

Une violation de données est un incident de sécurité au cours duquel des informations privées, confidentielles ou sensibles sont exposées ou dérobées sans autorisation. Les causes d'une violation peuvent varier, de l'erreur humaine à l'attaque malveillante, et les conséquences peuvent être graves. N'importe qui peut être victime d'une violation de données, surtout si ses comptes ne sont pas protégés.

Les violations de données peuvent entraîner:

Vol d'informations d'identification

Exemple: Des pirates ont obtenu un accès non autorisé à une base de données contenant les noms et les mots de passe des utilisateurs d'une plateforme de médias sociaux, ce qui a conduit à une prise de contrôle généralisée des comptes et à une utilisation abusive des informations personnelles.

Usurpation d'identité

Exemple: Un cybercriminel a utilisé des informations personnelles volées, telles que des numéros de sécurité sociale et des adresses, pour demander frauduleusement des prêts et des cartes de crédit au nom des victimes, ce qui a entraîné des dommages financiers et des complications de justification d'identité.

Compromission d'actifs

Exemple: Un logiciel malveillant a infecté le réseau d'une entreprise, en permettant aux attaquants de contrôler les systèmes critiques et les données sensibles, en perturbant les opérations et en causant des pertes financières importantes.

Fraude à la carte bancaire

Exemple: Une cyberattaque a visé le système de traitement des paiements d'un détaillant en ligne, entraînant le vol des informations de cartes bancaires des clients, informations ensuite utilisées pour effectuer des achats non autorisés.

Accès à des comptes

Exemple: Un fournisseur de services cloud a subi une violation de données permettant à des tiers non autorisés d'accéder à des fichiers et des informations sensibles stockés par ses clients, ce qui a entraîné la possibilité de fuites de données et de violations de vie privée.

Comment se produit une violation de données?

Les violations de données peuvent être un acte de cybercriminalité si elles sont commises de façon malveillante, mais il peut également s'agir d'une erreur involontaire de la part d'une personne disposant d'un accès autorisé aux données.

Les causes de violations de données sont les suivantes:

Malveillance d'un initié

Des personnes ayant accès à une base de données abusent intentionnellement de leurs droits d'accès pour dérober ou divulguer des informations sensibles.

Malveillance d'une personne extérieure

Une personne extérieure à l'organisation attaque une base de données par le biais d'un phishing, d'un logiciel malveillant, d'une attaque de vulnérabilité ou d'une attaque par déni de service.

Manipulation accidentelle d'un initié

Des personnes disposant d'un accès autorisé exposent accidentellement des données en raison d'erreurs ou de mesures de sécurité insuffisantes. Techniquement, il s'agit d'une fuite de données puisqu'il s'agit d'une erreur interne ; cependant, les conséquences sont les mêmes pour les personnes concernées et l'entreprise peut faire l'objet de poursuites judiciaires.

Les différentes phases d'une violation de données

Contrairement à ce qu'on pourrait imaginer, une violation de données malveillante n'implique généralement pas un individu vêtu de noir se faufilant la nuit dans un bâtiment avec une clé USB. Elle implique plutôt un groupe de personnes réfléchissant à distance à la manière de pirater une base de donnéese.

Les violations de données ne sont cependant pas toutes malveillantes. Certaines résultent d'une erreur humaine ou d'une négligence, et nous y reviendrons dans la section suivante.

Voici les trois étapes d'une violation de données intentionnelle.

1. La Recherche

Pour commencer, le pirate choisit une cible - généralement une entreprise ou une organisation ayant accès à des données personnelles - et cherche comment il pourrait s'infiltrer dans la base de données de sa cible.

Le pirate recueille des détails tels que des informations sur les employés, les dossiers financiers et les budgets de sécurité. Il recherche également des vulnérabilités telles que des mots de passe faibles, des logiciels obsolètes ou des connexions réseau non protégées.

2. L'attaque

En s'appuyant sur le résultat de ses recherches, l'attaquant peut maintenant s'attaquer au système de données. Voici quelques méthodes courantes utilisées par des pirates pour accéder aux systèmes ou aux réseaux de l'entreprise :

- **Le vol d'informations d'identification:**
  Ils collectent des noms d'utilisateur et des mots de passe compromis par le biais du dark web, de phishing, d'attaques par force brute ou même du vol physique d'appareils, afin de se faire passer pour des utilisateurs légitimes et de pouvoir accéder aux systèmes.

- **E-mails de phishing:**
  Les attaquants utilisent également des informations personnelles issues de leurs recherches, comme des titres de postes ou des noms de collègues, pour inciter leurs cibles à fournir des informations d'identification ou à cliquer sur un lien malveillant qui téléchargera un logiciel malveillant sur leur ordinateur.

- **Logiciels malveillants:**
  Les pirates utilisent des logiciels malveillants pour infecter secrètement l'ordinateur ou le réseau d'une victime et en prendre le contrôle afin de dérober des données.
- **Exploitation de vulnérabilités:**
  L'attaquant utilise des vulnérabilités telles que des mots de passe faibles, des configurations erronées ou des systèmes non corrigés découvertes dans le système informatique d'une entreprise pour y accéder.

- **Attaques par déni de service (DoS):**
  Cette attaque submerge un site Web avec un trafic factice excessif jusqu'à ce que le site soit indisponible pour les utilisateurs réels. Elle détourne ainsi l'attention d'autres faiblesses de sécurité pour permettre aux attaquants de procéder à des violations de données.

3. L'extraction de données

Après avoir accédé au système ou au réseau de la cible, les attaquants peuvent localiser et extraire des données précieuses ou sensibles, telles que des informations personnelles, des dossiers financiers ou toute autre donnée qu'ils pourront vendre sur le dark web.

Les données extraites sont alors copiées ou transférées sur les serveurs de l'attaquant, où celui-ci peut les contrôler et les exploiter. Souvent, une entreprise ne sait pas que ses données ont été dérobées jusqu'à ce qu'un tiers, comme les forces de l'ordre, les fournisseurs de services ou les clients, signale la violation.

04.
Comment vous protéger et protéger vos informations

Voici quelques moyens simples pour rester en sécurité en ligne. Panda Dome propose un plan de protection pour tous les types d'activités, de sorte que vous pouvez surfer en toute tranquillité.

Sécurité des réseaux

La sécurité des réseaux implique la mise en œuvre de mesures visant à protéger les réseaux informatiques contre les accès non autorisés, les cyberattaques et les violations de données. Il s'agit notamment de sécuriser l'infrastructure du réseau, de surveiller le trafic et de mettre en œuvre des protocoles de chiffrement robustes.

Utilisez les réseaux Wi-Fi publics en toute sécurité

Soyez prudent lorsque vous vous connectez à des réseaux Wi-Fi publics, afin d'éviter tout accès non autorisé à des données sensibles.

Servez-vous d'un VPN

Renforcez la confidentialité et la sécurité en ligne en chiffrant le trafic Internet lorsque vous accédez à des réseaux publics.

Installez un firewall

Mettez en place une barrière contre tout accès non autorisé à votre réseau, en ajoutant une couche supplémentaire de défense contre les cybermenacesproviding an additional layer of defense against cyberthreats.

Authentification et contrôle d'accès

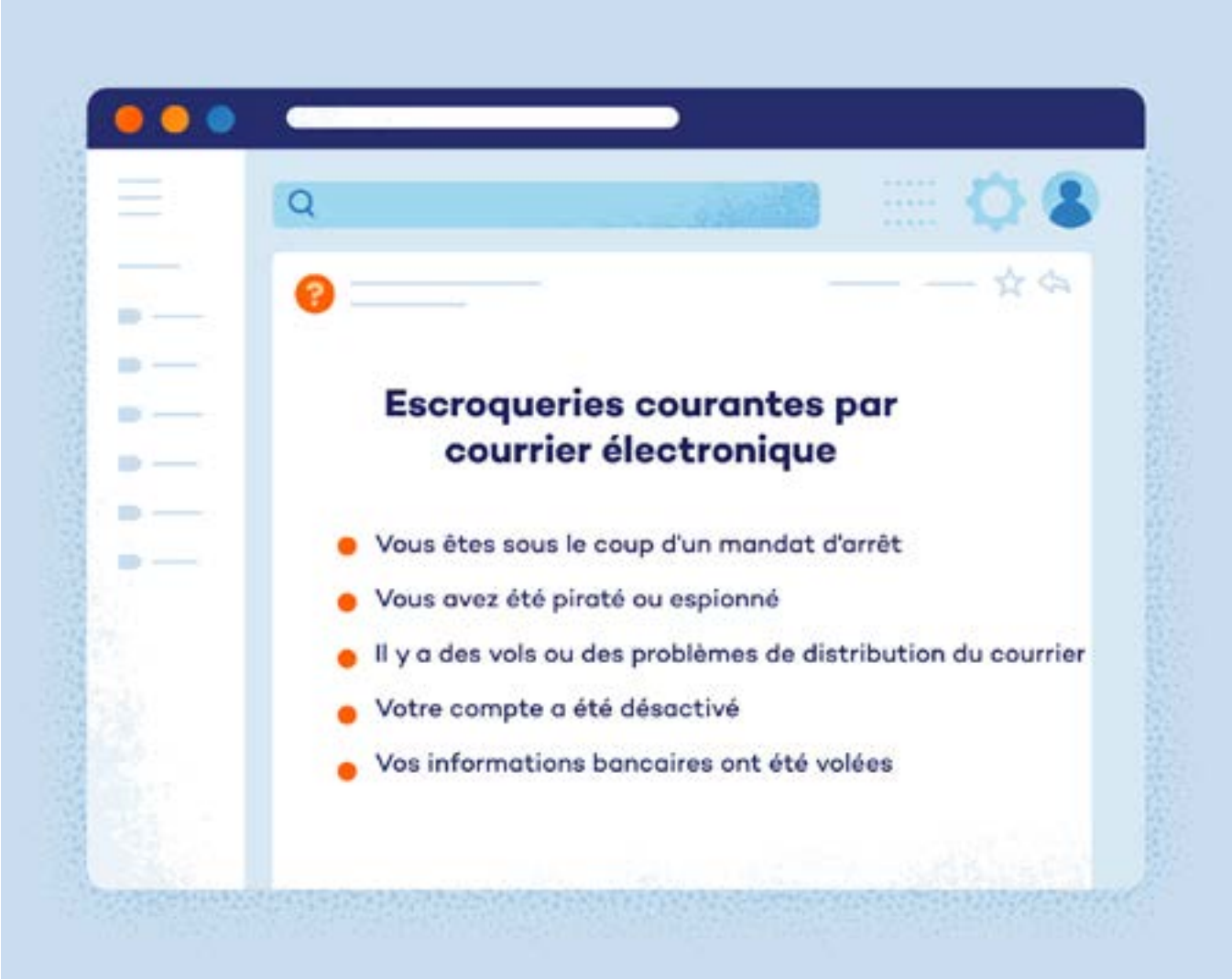
L'authentification et le contrôle d'accès sont des composantes essentielles de la confidentialité des données, car ils garantissent que seules les personnes ou les systèmes autorisés pourront accéder aux données ou aux ressources sensibles. Ces mesures permettent de vérifier l'identité des utilisateurs et d'appliquer des restrictions à leurs actions au sein d'un réseau ou d'un système.

- **Choisissez des mots de passe sûrs et uniques**
  Renforcez la sécurité de vos comptes en créant des mots de passe complexes et uniques pour chaque compte afin de réduire le risque d'accès non autorisé.

- **Mettez en place une authentification à deux facteurs**
  Ajoutez une couche de sécurité supplémentaire en exigeant une deuxième forme de vérification, telle qu'un code envoyé à un appareil de confiance, en plus du mot de passe.

- **Surveillez les comptes**
  Examinez régulièrement l'activité des comptes afin de détecter tout comportement suspect ou toute tentative d'accès non autorisé. Signalez rapidement toute activité suspecte ou tentative d'accès non autorisé aux autorités compétentes ou aux fournisseurs de services.

- **Ne communiquez jamais les codes reçus par SMS ou par courrier électronique**
  Évitez de partager les codes de vérification reçus par SMS ou par e-mail, car ils pourraient être interceptés par des pirates tentant d'obtenir un accès non autorisé.



Protection et récupération des données

Protection et récupération des données désignent les stratégies et technologies utilisées pour sauvegarder et restaurer les données en cas de suppression accidentelle, d'altération ou de cyberattaque. Il s'agit de mettre en œuvre des solutions de sauvegarde et des plans de chiffrement et de reprise après sinistre pour garantir l'intégrité et la disponibilité des données.

Sauvegardez vos données

Protégez-vous contre la perte de données due à des cyberattaques ou à des défaillances matérielles en sauvegardant de façon régulière vos fichiers et documents importants.

Installez un logiciel antivirus

Protégez-vous contre les logiciels malveillants et les autres cybermenaces en installant un logiciel antivirus fiable qui détectera et supprimera les logiciels malveillants de vos appareils.

Connaissances générales en matière de cybersécurité

Il est important de connaître les signes les plus courants de piratage afin de pouvoir agir le plus rapidement possible et récupérer vos comptes.

Voici quelques signes indiquant que vous avez peut-être été victime d'un piratage:

- L'utilisation d'Internet par l'appareil augmente considérablement
- L'appareil fonctionne plus lentement
- La batterie s'épuise rapidement sans explication
- Vous recevez des demandes non autorisées de changement de mot de passe
- De nouveaux logiciels ou de nouvelles applications sont téléchargés automatiquement

05.
FAQ sur la confidentialité des données

Cette section présente les réponses à quelques questions courantes sur la confidentialité des données

Quel est l'objectif de la loi sur la confidentialité des données?

L'objectif de la loi sur la confidentialité des données est de protéger les informations personnelles des individus en réglementant leur collecte, leur traitement et leur stockage, afin de favoriser la transparence et la protection des données.

Elle vise à établir des normes pour la collecte, l'utilisation, le traitement, le stockage et la suppression des informations personnelles..

Quels sont les 4 niveaux de confidentialité des données?

Les quatre niveaux de confidentialité des données correspondent à différents niveaux d'accès et de sensibilité:

Données publiques

Il s'agit d'informations destinées à une utilisation publique, telles que les coordonnées générales de l'entreprise, qui ne nécessitent généralement pas de protection stricte de la confidentialité.

Données internes

Il s'agit des données accessibles uniquement au sein de l'organisation, qui nécessitent généralement des mesures de protection pour empêcher l'accès non autorisé par des personnes externes.

Données confidentielles

Il s'agit d'informations sensibles qui nécessitent des mesures de confidentialité renforcées afin de limiter l'accès aux seules personnes autorisées au sein de l'organisation.

Données restreintes

Il s'agit de données très sensibles soumises à des contrôles stricts en matière de protection de la confidentialité, qui nécessitent souvent des autorisations spéciales pour l'accès et la manipulation afin de minimiser le risque d'exposition non autorisée ou d'utilisation abusive.

Quelles données sont considérées comme relevant de la vie privée?

Les données relatives à la vie privée, également connues sous le nom d'informations personnelles identifiables (IPI), sont toutes les informations qui permettent d'identifier directement ou indirectement une personne. Il s'agit notamment des données d'identité de base telles que le nom et la date de naissance, des informations de contact telles que les adresses électroniques et les numéros de téléphone, des données financières telles que les numéros de carte de crédit et des informations sensibles telles que les dossiers médicaux.