Shred-it®
Une Solution Stericycle®

Élimination sécurisée des données. Protéger les institutions financières et l'environnement.

Un guide sur la sécurité de l'information

Nous protégeons ce qui compte.

Sommaire.

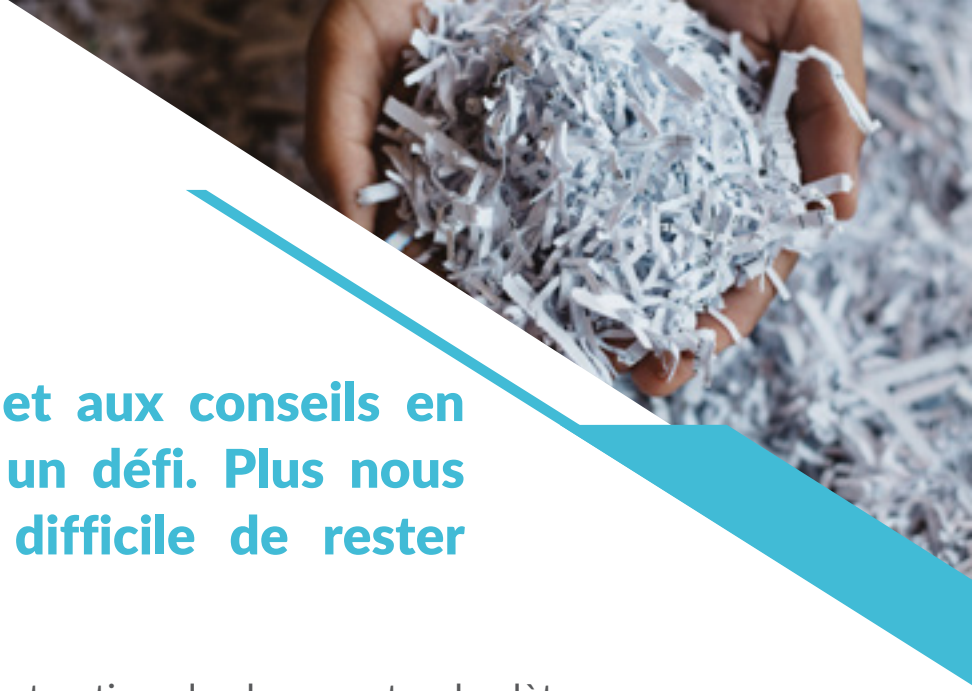
Introduction.

La protection des données sensibles est plus qu'une obligation légale.

Bien que nous so yons tous familiers avec la législation sur le RGPD et ses directives en constante évolution en matière de protection des données, en r aison du gr and nombre de documents en circulation au sein d'une institution financiere, décider ce qu'il faut détruire peut être un défi. Les risques peuvent être importants si les informations client ou commerciales sont stockées ou éliminées de manière incorrecte, ou si elles son t compromises.

Le stockage n'est pas toujours la solution pour rester en conformité. Découvrez les risques potentiels et les avantages liés à la sécurité de l'information, ainsi que la manière dont les institutions financières peuvent pleinement exploiter leur potentiel en tant que force progressive dans la lutte contre la crise climatique.

La loi et la destruction sécurisée des fichiers confidentiels.



Réagir rapidement aux évolutions législatives et aux conseils en matière de protection des données peut être un défi. Plus nous conservons d'informations, plus il peut être difficile de rester conforme.

Les nouveaux projets de loi et les orientations réglementaires en matière de traitement, de stockage et de protection des données personnelles des citoyens de l'UE et de la France peuvent rapidement impacter les processus internes de gestion des documents des institutions financières.

- La Loi sur la protection des données
- Le règlement général sur la protection des données (RGPD)
- La commission Nationale Informatique & Libertés (CNIL)
- Droit d'accès à ses données personnelles

Reporter la destruction de documents obsolètes, conserver des papiers indéfiniment ou les stocker, voire les éliminer dans des bacs de recyclage, peut exposer votre organisation aux violations de données et aux sanctions financières.

La Commission Nationale Informatique & Libertés (CNIL) recommande la destruction sécurisée pour éliminer les documents papier. En travaillant avec des professionnels de la destruction d'informations, vous vous assurez que votre organisation bénéficie d'une chaîne de contrôle sécurisée pour vos informations sensibles et qu'elle est en conformité avec les règles de protection des données en constante évolution.

Comprendre les risques

Les violations de données et le recyclage non sécurisé peuvent avoir un impact significatif sur votre activité.

Pertes financières

Les violations de données peuvent entraîner des pertes financières en raison du coût de la notification des personnes concernées ; des sanctions pécuniaires de la Commission nationale de l'informatique et des libertés ; et de la mise en conformité aux exigences réglementaires.

Atteinte à la réputation.

Outre l'interruption des activités, une violation de données pourrait réduire la confiance des clients et nuire à votre réputation.

Responsabilité juridique

Vos sites peuvent être tenus de verser une indemnisation aux personnes concernées par une violation de données.

Élimination non sécurisée.

Laisser des documents dans un bac de recyclage non sécurisé peut sembler respectueux de l'environnement, mais des informations importantes et confidentielles peuvent être compromises si elles sont récupérées dans ce bac.

Nous protégeons ce qui compte.

Erreurs de sécurité des données pouvant compromettre les informations confidentielles.

Les informations confidentielles stockées dans les livres comptables et les blocs-notes, les feuilles de calcul, etc. doivent être protégées contre les tiers malveillants et détruites lorsqu'elles ne sont plus nécessaires.

Laisser vos données exposées.

Protégez et sauvegardez toujours les informations privées lorsqu'elles sont visibles dans les espaces publics : par exemple, les informations sensibles non classées laissées sur les bureaux et les écrans d'ordinateurs portables clairement visibles par tous.

Accumuler des disques durs.

Au lieu de stocker ou de mettre au rebut vos anciens disques durs, clés USB, CD, etc., déchiquetez et détruisez vos supports numériques et électroniques en toute sécurité afin que toute récupération de données soit impossible.

Déchiqueteuses de bureau.

Les déchiqueteuses de bureau monopolisent le temps précieux d'un collaborateur et génèrent des coûts de manutention importants. De plus le risque que les collaborateurs aient accès à des documents hautement sensibles auxquels ils ne devraient normalement pas accéder est alors présent.

Manque de formation des collaborateurs.

D'après une étude[1], 58 % des entreprises expriment des inquiétudes quant à la possibilité que leurs employés ne soient pas pleinement informés des bonnes pratiques pour prévenir une violation de données. Contribuez à renforcer la compréhension du rôle de chaque employé dans le maintien de la sécurité de votre entreprise.

Défis auxquels font face les institutions financières.

La protection des informations sensibles devient de plus en plus complexe pour les entreprises, suscitant des préoccupations quant aux conséquences qu'une violation de données pourrait avoir sur leurs clients.

Une étude indépendante portant sur la perception de 500 chefs d'entreprise en France a mis en évidence des préoccupations concernant la sécurité des données sensibles et les risques potentiels de violations.

En ce qui concerne le RGPD et la conformité réglementaire, les personnes interrogées évoquent la complexité des réglementations et des exigences en matière de protection des données, tout en reconnaissant la nécessité impérieuse d'améliorer la sécurité des données.

Les résultats de l'étude ont révélé que :

87%

des personnes interrogées estiment qu'il est difficile de protéger les données sensibles de leur entreprise.

41%

des personnes interrogées ont été victimes d'une violation de données au sein de leur entreprise

64%

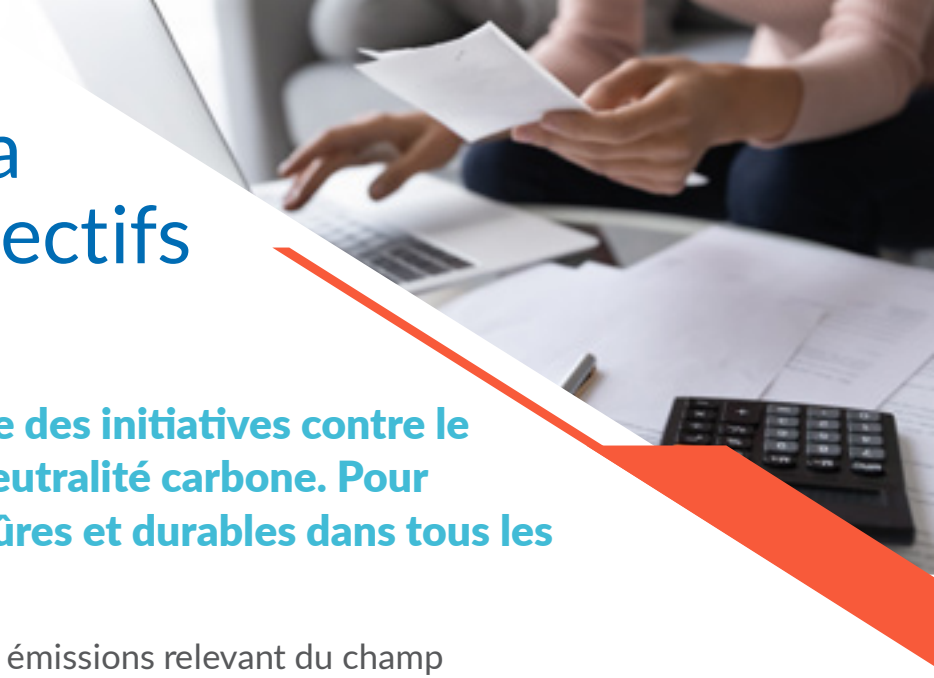
des personnes interrogées craignent que l'on n'accorde pas assez d'importance à la sécurité des informations physiques.

71%

craignent l'impact qu'une violation de données aura sur leurs clients

*Données internes à Shred-it

Développement durable: aligner la protection des données sur les objectifs de neutralité carbone.



La majorité des entreprises ont pour objectif de mettre en place des initiatives contre le changement climatique et de contribuer à la réalisation de la neutralité carbone. Pour atteindre ces objectifs, il est essentiel d'utiliser des pratiques sûres et durables dans tous les aspects du fonctionnement de l'entreprise.

La durabilité est fermement inscrite à l'ordre du jour national et le public se tourne de plus en plus vers les organisations pour aider à résoudre les problèmes environnementaux majeurs.

La loi française Climat et résilience vise à:

- Réduire les émissions de gaz à effet de serre d'au moins 55 % d'ici à 2030

L'une des façons dont les institutions financières cherchent à atteindre leurs ambitions de zéro émission nette consiste à adopter une stratégie scientifique à l'échelle de l'organisation qui favorise la réduction des émissions de gaz à effet de serre, à la fois au sein de l'organisation et dans l'ensemble de leurs chaînes d'approvisionnement.

La décarbonation est un parcours guidé par des plans de transition à l'échelle de l'industrie et de l'entreprise.

La lutte contre les émissions relevant du champ d'application 3 fait partie du défi. De nombreuses entreprises disposent désormais de politiques ESG qui détaillent les actions qu'elles entreprennent pour améliorer leurs résultats environnementaux.

La destruction et le recyclage sécurisés des données complètent les initiatives en matière de développement durable en faisant en sorte que le papier déchiqueté se retrouve dans l'économie circulaire. Les organisations peuvent respecter les réglementations en matière de protection des données et témoigner de leurs émissions relevant du champ d'application 3 relatives à la collecte et au déchiquetage du papier dans la catégorie Biens et services achetés.

Mesures concrètes : ce que vous pouvez faire dès maintenant.

Prenez des mesures immédiates pour protéger les informations confidentielles et intégrer des pratiques durables dans votre organisation. Explorez les points suivants qui peuvent faire l'objet d'une action :

Avis de confidentialité :

Élaborez un avis de confidentialité complet décrivant vos engagements en matière de protection des données et informant les individus de leurs droits. Expliquez comment et pendant combien de temps les données personnelles seront conservées avant d'être éliminées ou détruites, y compris celles figurant dans les dossiers papier.

Politique de conservation :

Gérez les dossiers physiques et expliquez le processus de suppression/ destruction.

Politiques sur le lieu de travail :

Mettez en œuvre des structures de travail robustes sensibilisant les employés à la sécurité de l'information. Favorisez une culture de responsabilité et de vigilance. Considérez la nécessité de politiques atténuant les risques de sécurité liés aux dossiers physiques.

Stockage sécurisé :

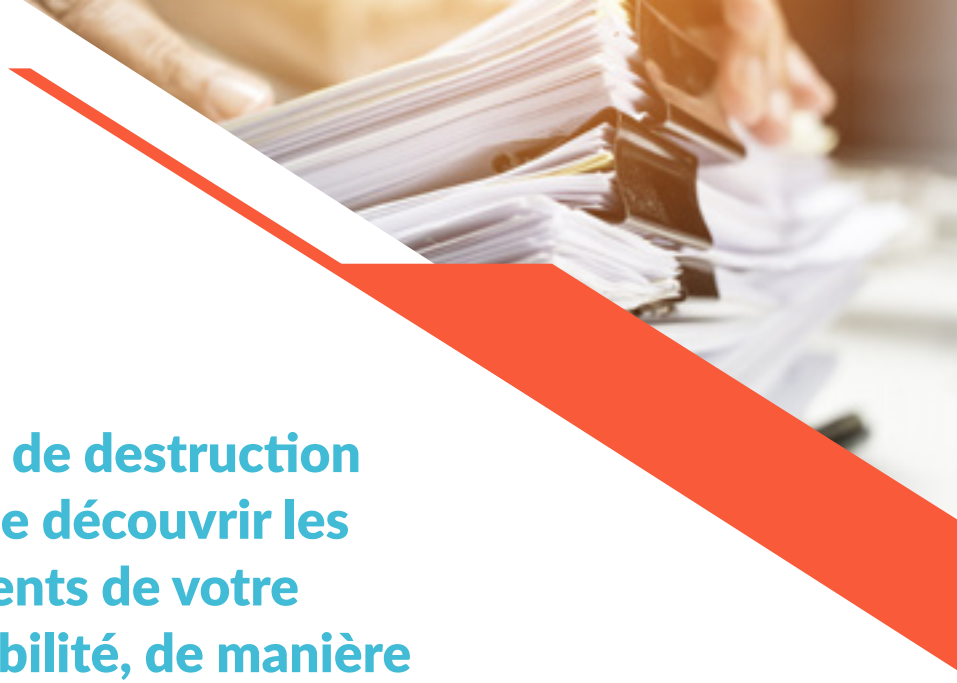
Protégez les informations sensibles en utilisant des solutions de stockage sécurisées comme des armoires fermées à clé, des zones d'accès restreint et un stockage numérique crypté. Tenez compte des risques liés aux différents supports tels que le papier ou les disques durs.

Formation du personnel :

Investissez dans des programmes complets de formation du personnel pour sensibiliserles employés aux meilleures pratiques en matière de sécurité de l'information. Donnez à votre personnel les moyens d'être la premiere barrière de protection et assurez-vous que les politiques et les normes sont mises en œuvre et respectées.

Destruction sécurisée :

Associez-vous à un fournisseur de services de destruction sécurisée de confiance, tel que Shred-it. Veillez à ce que vos documents confidentiels soient traités en toute sécurité, détruits de manière efficace et recyclés de manière responsable.



Comment un prestataire de services de destruction sécurisée peut vous aider

Une collaboration avec un prestataire de services de destruction sécurisée, tel que Shred-it, peut vous permettre de découvrir les meilleures pratiques en accord avec les engagements de votre organisation en matière de conformité et de durabilité, de manière rentable et sécurisée.

Services réguliers ou ponctuels

Déchiquetage sur site ou hors site

Chaîne de contrôle sécurisée

Certificat de destruction

Recyclage de l'ensemble du papier déchiqueté

Shred-it®
Une Solution Stericycle®

Appelez le **0800 844 848**

Visitez notre site web : **shredit.fr**

Contactez-nous dès aujourd'hui et franchissez la prochaine étape vers la construction d'un cadre de sécurité de l'information résilient qui contribue à protéger la réputation de votre organisation, maintient la confiance, assure la conformité et participe à votre démarche vers la neutralité carbone.

[1]:Rapport sur la protection des données Shred-it 2022

[2]: Données internes à Shred-it, 2022

Nous protégeons ce qui compte.