RGPD : STOCKAGE ET DESTRUCTION DE DOCUMENTS PAPIER

RGPD et conservation des documents : Meilleures pratiques pour les documents papier
Découvrez l'impact du RGPD sur la conservation des documents et apprenez les pratiques de destruction sécurisée et les outils de conformité pour les entreprises.

RECOMMANDÉ PAR LE COACH FELLOWES DE LA VIE DU BUREAU

Le Règlement général européen sur la protection des données (RGPD), promulgué le 25 mai 2018, a entraîné des changements importants dans la manière dont les entreprises gèrent les données à caractère personnel, en étendant sa compétence des autorités publiques aux petites et moyennes entreprises. Le RGPD énonce des règles strictes pour le traitement des données à caractère personnel, couvrant des informations telles que les noms, les adresses, les adresses e-mail, les numéros de sécurité sociale, et plus encore. Le non-respect de ces règles peut entraîner des amendes allant jusqu'à 4 % du chiffre d'affaires mondial ou 20 millions d'euros, ce qui souligne la nécessité pour les entreprises de donner la priorité à la protection des données.

RGPD et conservation des documents : meilleures pratiques pour les documents papier

Pour se conformer au RGPD, les entreprises doivent étendre leurs politiques de protection des données aux documents papier. Qu'ils soient stockés sous forme électronique ou sur papier, les organisations doivent mettre en œuvre des mesures techniques et organisationnelles pour garantir un traitement sécurisé des données. Les principaux éléments à prendre en compte pour les documents papier dans le cadre du RGPD sont les suivants :

- **Destruction sécurisée :** les documents contenant des données dont on n'a plus besoin doivent être détruits en toute sécurité par des méthodes telles que le déchiquetage.
- **Stockage :** les documents qui doivent être conservés doivent être stockés de manière à permettre une traçabilité et une accessibilité aisées en cas de besoin.
- **Contrôle d'accès :** les documents sensibles doivent être stockés dans des armoires fermées à clé, avec un accès restreint limité au personnel autorisé.
- **Inclure les employés à distance :** Les politiques doivent englober les collaborateurs temporaires et ceux à distance en décrivant les procédures de protection des documents et des données en leur possession.

Principes de protection des données

Chaque stratégie de protection des données doit respecter les principes selon lesquels les données sont :

1. Traitées de manière légale, équitable et transparente
2. Collectées à des fins spécifiques, explicites et légitimes, et non traitées ultérieurement d'une manière contraire à ces fins
3. Adéquates, pertinentes et limitées à ce qui est nécessaire
4. Exactes et à jour. Les erreurs doivent être traitées, supprimées et corrigées
5. Conservées pendant une durée n'excédant pas celle qui est nécessaire
6. Traitées de manière sécurisée

Nous avons vu qu'un principe fondamental du RGPD est que les données ne doivent pas être conservées plus longtemps que nécessaire et soient éliminées en toute sécurité. Nous verrons ci-dessous pourquoi le déchiquetage est si important pour se conformer au RGPD.

Destruction sécurisé et RGPD : ce que vous devez savoir

Vos documents ne sont pas en sécurité tant qu'ils n'ont pas été détruits !

Chaque organisation a la responsabilité légale de protéger les informations sensibles et d'éliminer le matériel confidentiel en toute sécurité. L'organisation est également responsable de tout matériel confidentiel emporté en dehors de ses locaux par l'un de ses employés. Il s'agit à la fois des documents imprimés et de tout ce qui peut être consulté sur un ordinateur portable ou de bureau, ou un appareil mobile.

Malgré une sensibilisation accrue à l'usurpation d'identité au cours des dernières années, celle-ci continue de se développer à un rythme alarmant en France. Et comme nous traitons quotidiennement un grand nombre d'informations, nous sommes tous exposés au risque, que ce soit en tant que particuliers ou entreprises.

Un relevé bancaire jeté au rebut, une bribe d'information sur les salaires ou une proposition de client froissée peuvent suffire à un criminel pour vous causer des dommages irréparables, à vous et à votre entreprise.

Trois conseils pour de meilleures pratiques de destruction

Une destruction sécurisée est essentielle pour éviter que des documents confidentiels ne tombent entre de mauvaises mains et pour réduire l'exposition de l'organisation à des violations de données. Utiliser une déchiqueteuse pour détruire en toute sécurité des documents confidentiels devrait faire partie de notre routine quotidienne, où que nous travaillions.

- Ne partez pas du principe que tout le monde comprend le RGPD. Formez tous les employés aux exigences du RGPD, au traitement des données personnelles et aux 6 principes de la protection des données. Cette formation doit être dispensée à tous les nouveaux arrivants, à chaque fois que la législation est mise à jour, et dans le cadre de séances régulières de remise à niveau portant sur la sécurité des données.

- Détruisez tous les papiers sensibles avant de les recycler ou de les mettre au rebut, idéalement sans prendre le risque de les transporter de chez vous au bureau, ou inversement.

- Donnez à tous les employés un accès facile à une déchiqueteuse sécurisée à domicile et au travail pour garantir la conformité au RGPD partout où votre équipe travaille.

Le déchiquetage est de loin le meilleur moyen de détruire en toute sécurité des documents confidentiels pour protéger les informations commerciales sensibles et les identités personnelles.

Agissez dès aujourd'hui pour protéger votre entreprise.