



Le travail hybride fait-il courir de plus grands risques de violation des données aux entreprises ?

Fellowes

Étude 2022 sur la protection des données. Un rapport sur la destruction de documents dans un environnement de travail hybride.

Avant-propos



“ De nombreuses entreprises qui sont passées à un modèle de télétravail au début de l'année 2020 ont découvert qu'elles n'avaient simplement pas eu assez de temps pour réaliser les évaluations des risques avant d'appliquer ces changements drastiques à leurs méthodes de travail ”

“Chacun s'est concentré sur le maintien de ses services plutôt que sur l'étude des risques associés aux changements. Les employés n'ont pas non plus eu le temps de s'adapter à la nouvelle méthode de travail. Plusieurs études ont mis en lumière les mauvaises habitudes en matière de sécurité des données qui avaient été repérées au cours de la pandémie pendant les périodes de télétravail.

En 2022, la manière dont nous travaillons a rapidement évolué, nous sommes de plus en plus nombreux à adopter un mode de travail hybride dans le cadre du retour au bureau post-pandémie. Mais les entreprises ont-elles agi et les procédures ont-elles été adaptées ? Ou le nouveau mode de travail fait-il courir davantage de risques de violation des données aux entreprises ?

La réponse à la deuxième question est « Oui ». La moitié des participants de l'étude pensent que le travail hybride peut avoir augmenté la quantité de données sensibles perdues ou violant les règles du RGPD. La gestion des documents papier n'était pas ce qui inquiétait le plus les entreprises en matière de politique de sécurité. Cependant, la transition rapide au mode de travail hybride signifiait que des milliers de documents supplémentaires étaient transportés entre le domicile et le bureau chaque semaine. Cela pose des questions importantes en termes de confidentialité des documents et sur la manière dont nous les protégeons, dans un monde où nombre d'employés ne travaillent plus seulement au bureau.

Pour s'appuyer sur les 40 ans d'expertise de Fellowes dans le secteur des destructeurs, nous voulions découvrir comment les individus sécurisent et détruisent les documents dans un monde où le travail hybride se développe de plus en plus. Nous voulions également découvrir comment les entreprises se conforment au RGPD (Règlement Général sur la Protection des Données), 4 ans après son entrée en vigueur. Dès le début, nous avons développé des destructeurs pour qu'ils répondent aux besoins de tous les lieux de travail. Nous nous engageons à protéger les entreprises et les particuliers où qu'ils travaillent, en empêchant que des documents papier ne tombent entre de mauvaises mains.

Nos recherches, en partenariat avec B2B International, ont visé 605 utilisateurs de destructeurs en France, en Allemagne et au Royaume-Uni, travaillant dans les services financiers, le secteur public et la santé.

Dans ce rapport, nous allons étudier les tendances et comportements relatifs à la sécurité des données dans cet environnement de travail en constante évolution et nous espérons que nous pourrions guider les entreprises dans cette phase de changement. Quel que soit le lieu où vous travaillez, la destruction de documents sensibles est essentielle pour maîtriser les risques auxquels chaque entreprise doit faire face en matière de sécurité.”

Steven Hickey

Responsable Marketing Européen - Workspace solutions

Frise chronologique sur l'évolution des destructeurs

1982

Destructeurs commerciaux

Fellowes conclut un accord de licence avec une entreprise allemande pour la production de destructeurs commerciaux



1990

Le premier destructeur personnel

Une invention, le destructeur de papier individuel, est dévoilée



2005

SafeSense™

Présentation de la technologie SafeSense™ de Fellowes qui rend les destructeurs plus sûrs pour une utilisation à domicile



2008

Destructeurs anti-bourrage

Présentation de la gamme de destructeurs Fellowes 100% anti-bourrage pour éviter les bourrages papier dans les destructeurs de documents



2014

Destructeurs AutoMax™ à alimentation automatique

Fellowes présente les destructeurs AutoMax™ à alimentation automatique pour améliorer la productivité du destructeur au bureau



2020

LX Series

Présentation des nouveaux destructeurs à microparticules de Fellowes, conçus pour s'adapter à tous les espaces de travail



RGPD et protection des données dans un monde professionnel hybride

Nos recherches ont montré que **8 personnes interrogées sur 10** ont adopté le télétravail, qu'il soit partiel ou total. Le travail hybride est une combinaison de travail sur site et à distance. Il peut offrir de la flexibilité et du choix en terme de lieu de travail, mais il présente le défi quotidien de veiller à ce que les individus aient conscience de la confidentialité des documents qu'ils transportent avec eux. Il faut également qu'ils appliquent les principes de protection des données où qu'ils soient.



Que vos employés travaillent au bureau, chez eux ou dans des espaces de travail partagés, vous devez gérer les risques en matière de sécurité des données. Cela commence par vous assurer que vous étudiez tous les environnements qui peuvent poser de nouveaux risques à votre entreprise. Par exemple, vous devez avoir des politiques strictes à imposer à vos employés pour ce qui est de l'utilisation de leurs propres ordinateurs, tablettes et smartphones à des fins professionnelles, car vous aurez moins de contrôle sur la manière dont ces appareils sont configurés et utilisés. Un autre point d'inquiétude est l'utilisation du Wi-Fi (public et à domicile), ainsi que des mots de passe qui peuvent être faibles et utilisés plusieurs fois. Ce sont là deux points d'intrusion pour les cyber-attaques et des instructions claires doivent être données aux employés afin de s'assurer que ces derniers soient protégés.

Sans surprise, les documents papier constituent l'un des risques les plus sous-estimés pour les entreprises. Tout étant aujourd'hui numérisé, les individus oublient souvent d'inclure les données papier dans leur politique de sécurité. Il est toutefois important de souligner que la majorité des entreprises (68 %) ayant participé à notre étude, ont indiqué qu'elles géraient quotidiennement une grande quantité de données papier sensibles.

Vous n'êtes pas sûr de connaître les détails du RGPD ? Nous sommes là pour vous...

Le Règlement Général sur la Protection des Données (RGPD) a été présenté en mai 2018 et constitue un ensemble complet d'exigences en matière de protection des données pour le traitement des données personnelles des citoyens européens. Toute organisation manipulant ces données personnelles doit les collecter uniquement sous des conditions strictes, pour des finalités légitimes, et les protéger contre tout usage abusif.

Les données personnelles doivent être traitées de manière à garantir leur sécurité, notamment contre tout traitement non autorisé ou illégal, ainsi que contre la perte, la destruction ou l'altération accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Qu'est-ce que les données personnelles ?

Les données personnelles sont des informations relatives à une personne vivante pouvant être identifiée à partir de ces données. Cela peut inclure des noms, adresses, numéros de sécurité sociale, informations issues des réseaux sociaux, images de vidéosurveillance (CCTV) ou photographies. Les données personnelles peuvent être sous format numérique ou papier.

Quelles sont les conséquences en cas de non-conformité au RGPD ?

Une violation des données personnelles peut entraîner des amendes pouvant aller jusqu'à **4 % du chiffre d'affaires mondial ou 20 millions d'euros**, ainsi qu'une atteinte à la réputation de l'entreprise.

Les six principes de la protection des données

Chaque stratégie de protection des données doit inclure les principes suivants :

- ▶ **Traitement légal, équitable et transparent**
- ▶ **Collecte à des fins spécifiques, explicites et légitimes, sans traitement ultérieur contraire à ces objectifs**
- ▶ **Données adéquates, pertinentes et limitées à ce qui est nécessaire**
- ▶ **Exactitude et mise à jour des données. Toute inexactitude doit être corrigée, effacée ou rectifiée**
- ▶ **Conservation limitée dans le temps, uniquement pendant la durée nécessaire**
- ▶ **Traitement sécurisé des données**

Découvrez-en plus sur le Règlement Général sur la Protection des Données (RGPD) - Fellowes®

70 % des personnes interrogées ont déjà emporté des documents professionnels chez eux, imprimé des documents professionnels à leur domicile, ou les deux. Et presque la moitié d'entre eux ont ensuite placé ces documents dans une corbeille ou un bac de recyclage sans les détruire. De plus, **46 %** des personnes interrogées ont été témoins de documents confidentiels laissés sans surveillance. Cela doit être une préoccupation pour les entreprises. Même s'il semble y avoir des politiques strictes relatives à la destruction des données sensibles au sein des entreprises européennes, ces directives ne sont pas souvent respectées en dehors du bureau. Que ce soit dans un bureau ou au domicile, les données sensibles doivent être placées sous clé quand elles ne sont pas utilisées et détruites en toute sécurité une fois qu'elles ne sont plus utiles aux fins pour lesquelles elles ont été acquises.

Notre étude a également révélé que même après 4 ans, seuls **60 %** des individus connaissent le RGPD, et seulement **1 entreprise sur 4** a adapté ses politiques afin d'y inclure le travail à domicile. Les organismes comme la Commission Nationale de l'Informatique et des Libertés (CNIL) ont de nouveaux seuils de tolérance par rapport à la pression que les entreprises ont subi pendant la pandémie. Toutefois, la plupart des restrictions étant levées en Europe, la CNIL va devenir moins tolérante. Il est donc essentiel d'agir maintenant si vous souhaitez rendre le travail hybride permanent. Vous devez veiller à ce que ces politiques

soient révisées et mises à jour afin de refléter le nouveau mode de travail et couvrir les potentiels risques de violation des données.

Une fois ces politiques mises à jour, il est important d'avoir un plan robuste de mise en œuvre et de communication. L'étude a montré un décalage clair au sein des entreprises en fonction du niveau de hiérarchie. Alors que la majorité (83 %) des personnes interrogées occupant des postes senior semblait avoir conscience du RGPD et suivait activement les règles et règlements de l'entreprise relatives à la protection des données, seules **57 %** des personnes interrogées et occupant des postes junior connaissaient le RGPD et par conséquent, ne suivaient pas les directives, quel que soit leur lieu de travail.



La communication et le contrôle des données et documents sensibles semblent plus aisés dans le cas où tout le monde travaille ensemble au bureau. Mais le fait est que le travail hybride est là et les entreprises doivent l'adopter pour soutenir leurs employés. En parallèle, il est impératif que les procédures et règlements soient adaptés pour refléter ces changements. Les conséquences de la perte de documents papier sensibles sont considérables. Il est donc essentiel de former tous les employés à ces réglementations, à chaque niveau de l'entreprise, puisqu'il suffit de perdre une seule donnée pour entraîner une violation. Dans la partie suivante, nous proposerons des solutions pour mettre en œuvre ces changements dans l'entreprise.



ÊTRE CONFORME
AU RGPD



Que peuvent faire les entreprises pour aider leurs employés à se conformer aux politiques relatives aux données et à la confidentialité ?

Mise à jour des politiques

Vérifiez la politique "Apportez Votre Equipement personnel de Communication" (AVEC) : il s'agit d'une politique qui permet aux employés d'une organisation d'utiliser leurs appareils personnels pour des activités liées au travail.



Considérez le Wi-Fi public et celui du domicile privé comme une menace et expliquez à votre personnel ce qu'il doit faire pour les utiliser en toute sécurité.



Réviser et adapter vos politiques relatives à l'impression, au stockage et à la destruction des documents papier et ajoutez-y une partie sur le stockage et la destruction des documents en cas de télétravail.



Réviser vos politiques en matière de sécurité des mots de passe. L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) recommande d'utiliser des phrases avec trois mots plutôt que des mots de passe. Vous devez en outre envisager l'authentification à plusieurs facteurs.



Votre politique doit indiquer qu'avant de détruire, vendre ou donner un ancien ordinateur ou disque dur, toutes les données doivent être totalement supprimées.



Formation

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. La formation doit être donnée à tous les nouveaux arrivants et dans le cadre de séances régulières de remise à niveau portant sur la sécurité des données.



Fournissez une liste à vos employés des domaines / sites web qui pourraient poser un risque de violation des données. Vous pourriez également les laisser faire un Contrôle de la sécurité des données.



Veillez à ce que votre formation aborde le sujet des documents papier et la manière de les traiter. Informez sur quels documents et registres doivent être conservés, et lesquels doivent être détruits immédiatement après qu'ils cessent d'être utiles.



Ajoutez un module de formation sur la sécurité des données en télétravail, qui met en lumière les nouveaux ajouts apportés à vos politiques.



Envisagez un portail de formation en ligne afin de pouvoir suivre le statut de la formation de chacun.



Équipement

Afin d'éviter des problèmes avec la politique AVEC, nous conseillons à l'entreprise d'investir dans des ordinateurs portables plutôt que des ordinateurs de bureau. L'équipement pourrait ainsi facilement être transporté entre le domicile et le bureau.



Investissez dans des anti-virus et des pare-feu de niveau supérieur.



Veillez à ce que votre personnel ait accès à un destructeur dans les bureaux de l'entreprise et que les employés en télétravail soient équipés d'un petit destructeur.



Pour les données personnelles ou les données hautement confidentielles comme les adresses, factures et bilans, optez pour un destructeur à coupe microparticules (P-5) car la taille des particules de papier offre une sécurité supplémentaire en rendant les données impossibles à lire ou à reconstituer.



Garantissez un lieu de travail sûr et productif à vos employés en vous équipant de destructeurs de documents. Lors de l'achat prenez en compte le niveau de sécurité recherché.



Communication

La communication est essentielle à tous les niveaux de l'entreprise. Lutte contre le manque de connaissance des plus jeunes.



La sécurité des données sera abordée lors de vos prochaines réunions sur site, ainsi qu'en plus petits groupes lors des réunions mensuelles d'équipe ou des entretiens personnalisés.



Affichez des posters de rappel dans l'entreprise, mais intégrez également la mise à jour des politiques à votre newsletter et postez-la sur l'intranet.



Partagez les bonnes pratiques et exemples de menace d'hameçonnage ou de cyber-attaque avec vos employés afin que chacun puisse être vigilant.



Intégrez la sécurité des données à vos examens trimestriels d'entreprise.



Que peuvent faire les employés pour éviter la violation des données ?



Identifier les données sensibles et les protéger

Tout document contenant des données personnelles, ainsi que des registres commerciaux, doit être détruit en toute sécurité conformément aux exigences légales relatives à la conservation des données.



Renseignez-vous sur les délais de conservation des contrats, accords commerciaux et autres documents de ce type. Une fois ces conditions de conservation respectées, procédez à la destruction des papiers pour libérer de l'espace de stockage et assurer la confidentialité.



Les reçus, bordereaux de dépôt et relevés de compte peuvent généralement être détruits une fois qu'ils ont été utilisés.



Les registres des RH doivent être régulièrement contrôlés et une fois qu'ils ont atteint leur date légale d'expiration, ils doivent être détruits. Le RGPD veut que les services RH justifient s'ils conservent des données sur les employés (anciens ou actuels) et pourquoi ils conservent toute donnée au-delà de la durée de conservation obligatoire.



Stocker ou détruire des données papier en toute sécurité

Réfléchissez avant d'imprimer. Posez-vous la question : ai-je vraiment besoin d'une copie papier de ce document ? Qui pourrait accidentellement prendre ce document ?



Détruisez au fur et à mesure. Si cela n'est pas possible, détruisez tous les documents sensibles avant de les recycler ou les jeter, idéalement sans avoir besoin de prendre le risque de les transporter de chez vous au bureau, ou inversement.



Ne jamais laisser de données sensibles traîner sans surveillance, que ce soit à la maison ou au bureau. Rangez toujours votre bureau le soir, et placez les documents confidentiels sous clé, ainsi que tout accessoire informatique amovible avant de quitter votre poste de travail.



Réviser régulièrement les données que vous détenez et lorsque cela est possible, rendez les données personnelles anonymes dès qu'elles ne sont plus utiles.



Rester informé des formations et de la législation

Assurez-vous que vous connaissez les modules de formation existants et que vous y avez accès. Envisagez également de programmer des rappels trimestriels dans votre calendrier pour participer à des séances de remise à niveau.



Encouragez les collègues et membres de l'équipe à participer à des formations et rappelez-vous mutuellement les règles et directives si vous remarquez que quelqu'un n'agit pas dans le respect de la politique (ex. en laissant des documents sensibles traîner, en utilisant des périphériques personnels, etc.).



Familiarisez-vous avec les six principes de la protection des données.



Si vous avez des questions, parlez-en à votre responsable de la protection des données.



Ce qu'il faut retenir de notre étude

8 sur 10

ont adopté le travail à domicile

70%

des interrogés

ont déjà emporté des documents professionnels chez eux, imprimé des documents professionnels à leur domicile, ou les deux

47%

ne détruisent pas les documents professionnels après les avoir utilisés

>>> Augmentation du risque de perte des données pendant le transport !

46%

ont été témoins de documents confidentiels laissés sans surveillance

Manque de sensibilisation sur l'importance du RGPD chez les jeunes ou les postes junior seulement

57%

se disent familiers avec la réglementation

Après 4 ans seulement

60%

des personnes interrogées disent connaître le RGPD

41%

n'ont toujours pas eu de formation officielle sur le règlement RGPD pour le travail à domicile

Conseils pour de meilleures pratiques de destruction :

La destruction sécurisée est essentielle pour éviter que les documents confidentiels ne tombent entre de mauvaises mains cela permet également de réduire l'exposition de l'entreprise aux violations de données. Nous sommes à une époque où de plus en plus de personnes travaillent de manière hybride. Tout en se conformant au RGPD les risques que cela représente pour la sécurité des données sont évidents.

L'utilisation d'un destructeur de documents pour détruire en toute sécurité les documents confidentiels devrait faire partie de notre quotidien, partout où nous travaillons.

- ▶ Ne considérez pas que tous les individus comprennent le RGPD. Formez tous les employés aux règles du RGPD, au traitement des données personnelles et aux six principes de la protection des données. Cette formation doit être dispensée à tous les nouveaux arrivants, chaque fois que la législation est mise à jour, et dans le cadre de sessions régulières de mise à jour de la sécurité des données.
- ▶ Mettez sous clé les documents confidentiels lorsqu'ils ne servent pas et ne les laissez jamais sans surveillance à la maison ou au bureau.
- ▶ Détruisez tous les documents sensibles avant de les recycler ou de les détruire, idéalement sans prendre le risque de les transporter de la maison au bureau ou inversement.
- ▶ Donnez à tous les employés un accès immédiat à un destructeur de documents sécurisé à leur domicile et au travail.



Trouvez le destructeur adapté à votre environnement de travail.
Visitez www.Fellowes.com ou cliquez [ici](#)



Étude 2022 Respect de la confidentialité

Méthodologie

Cette étude a été menée par B2B International en avril 2022. 605 utilisateurs de destructeurs ont été interrogés, également répartis entre le Royaume-Uni, la France et l'Allemagne. L'accent a été mis sur les utilisateurs de destructeurs à différents niveaux d'ancienneté dans les petites et moyennes entreprises des secteurs suivants : services financiers (206), secteur public (206) et santé/médical (193).

Pour pouvoir comparer les habitudes de travail en matière de sécurité des données dans un monde professionnel hybride, il était important d'avoir une répartition égale entre les personnes travaillant à la maison et au bureau, travaillant principalement dans un bureau d'entreprise, uniquement dans un bureau d'entreprise, principalement à la maison ou uniquement à la maison.

Pour en savoir plus sur la méthodologie de répartition, n'hésitez pas à envoyer un e-mail à jdettler-bates@fellowes.com

Fellowes