9. Clés USB : une pratique à risque ?
Pour éviter de transporter son PC, une clé USB ou un petit disque externe peut être utile. Mais interrogez-vous quand même sur les fichiers que vous y transférez. S'il s'agit de retravailler à la maison une présentation PowerPoint, rien de grave. Mais s'il s'agit de données personnelles ou sensibles, vous prenez un risque en cas de perte, surtout si la clé n'est pas sécurisée. « Un responsable d'une agence web m'a expliqué qu'il gardait sur sa clé USB tous les *logins* et mots de passe de ses clients. C'est évidemment très risqué », avertit Damien Jacob. Certaines entreprises, qui manipulent des données sensibles, ont décidé d'interdire l'usage des clés USB. Il ne sera pas toujours nécessaire d'arriver à une telle extrémité : de simples directives aux membres du personnel sur les données qu'ils peuvent transporter à l'extérieur de l'entreprise peuvent suffire.

10. Faut-il fermer les pages Facebook professionnelles ?
Certaines pages Facebook professionnelles sont utilisées pour communiquer sur la vie de l'entreprise : nouveaux engagements, nouveaux projets, événements professionnels, conférences, journée du personnel, etc. Autant de publications qui peuvent amener à partager des données privées (nom d'un employé, profil Facebook, photo, âge, etc.). Problème : le réseau social est dans le collimateur des autorités européennes pour la légèreté avec laquelle il traite les données. « Facebook n'offre pas les garanties suffisantes en matière de confidentialité des données. Toutes les données qui concernent le personnel devraient donc être publiées en interne, par exemple sur l'Intranet de l'entreprise », estime Olivier Rijckaert, avocat spécialisé en droit du travail et fondateur de Sotra. Rien n'empêche cependant de conserver la page Facebook comme vitrine de l'entreprise, où les clients et prospects pourront obtenir toutes les informations nécessaires sur les produits et services qu'elle propose.

11. Des pseudos pour tout le monde ?
La « pseudonymisation » est une technique renseignée dans le RGPD pour garantir l'anonymat de certaines personnes et donc, la protection de leurs données personnelles. C'est ce que Gail Bajraktari, consultant chez Dynafin, conseille à certains de ses clients actifs dans le secteur financier. Les courtiers ou les filiales belges de banques étrangères sont en effet en possession de données dites « sensibles » qu'il convient de traiter avec la plus grande prudence. « Concrètement, la pseudonymisation consiste à séparer les données de leurs propriétaires respectifs pour que tout lien avec une identité ne soit possible sans une clé d'identification », pointe Gail Bajraktari.

12. Tout archiver… ou tout passer à la déchiqueteuse ?
Empiler les archives, c'est s'exposer au risque de conserver inutilement des données personnelles. Il ne sert cependant à rien d'être parano et de détruire systématiquement tous les documents après utilisation. Tout dépendra du type de données concernées. Une PME active dans le recrutement vient ainsi de commander de nouvelles déchiqueteuses afin d'éviter de laisser traîner des documents contenant des données personnelles. Mais l'entreprise s'interroge encore sur le sort à réserver aux C.V. de personnes non sollicitées pendant plusieurs années : « Nous sommes encore en réflexion à ce sujet, expose le *data protection officer* de la PME. Certains profils sont peu demandés, puis des années plus tard, une offre surgit. Ce serait dommage de ne plus les avoir en stock parce qu'on aurait décidé de les supprimer après quatre ans, par exemple. » Il peut donc être justifié de conserver, de manière sécurisée, certains documents pendant plusieurs années. Par contre, d'autres devraient être détruits rapidement. C'est le cas, par exemple, des certificats médicaux, qui contiennent des données de santé sensibles que l'employeur n'a aucune utilité à conserver.

13. Centres d'appels hors Europe : faut-il couper les ponts ?
Le RGPD s'applique à toutes les données personnelles de particuliers basés en Europe. Si vous faites appel à des co-contractants étrangers, vous devez vous assurer que ceux-ci sont en ordre, même s'ils sont situés hors du continent européen. Or, certains d'entre eux ne se sont pas encore mis en conformité. Faut-il pour autant couper les ponts avec, par exemple, un *call center* situé en Afrique ? « Les grandes entreprises sont en train de se désengager de leurs liens avec certains *call centers* situés hors Europe parce qu'elles estiment qu'ils ne sont pas en ordre. Nous suggérons aux PME de trouver une solution transitoire via des structures situées sur le continent européen », avance Anne Mikusinski, chargée de programme RGPD à l'UCM. La même

Une plateforme pour aider les PME à appliquer le RGPD

Depuis la mise en place du Règlement général sur la protection des données (RGPD), les entreprises et administrations se retrouvent avec une charge de travail administratif supplémentaire. Pour assurer cette mission difficile pour une PME, la start-up IDlegcy propose leur aide.

Partager un nouveau statut sur Facebook, s'inscrire sur un site web, utiliser des applications, compléter un formulaire pour recevoir une carte de fidélité… toutes ces activités génèrent des données que les entreprises et les administrations récoltent et utilisent, notamment à des fins publicitaires. Le RGPD donne un nouveau cadre pour la détention et l'utilisation de ces informations. Et les PME sont concernées au même titre que les géants du Web, les multinationales et les grandes entreprises.

Le RGPD impose notamment la présence d'un « data protection officer » (DPO) dans chaque entreprise et administration. Dans les grandes entreprises, un collaborateur prend généralement ce rôle à temps plein, et est parfois secondé par des collègues. Mais pour les petites entreprises, le DPO par défaut, c'est le gérant, qui se voit donc confronté une charge de travail administratif supplémentaire.