

Rappels d'ailleurs la définition au sens RGPD des « données à caractère personnel » : il s'agit de toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »). Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

peuvent être celles des salariés, des clients ou prospects, des fournisseurs ou partenaires. En ce sens, le RGPD stipule des objectifs à atteindre :

- le personnel pouvant y avoir accès.
- garantir un niveau de sécurité adapté au risque incluant chiffrage « au repos » ou pendant un transfert (art.32).
- définir des personnes habilitées pouvant avoir accès aux contenus avec données personnelles (art.29).
- définir un contrôle d'accès aux contenus avec données personnelles (art.25).
- auditabilité.
- protection contre destruction, perte, altération, diffusion ou accès non autorisés.

comme l'obligation de rendre publique tout vol de données personnelles, la désignation de « DPO », le droit à l'oubli...

d'information et des usages actuels ne sont pas "compatibles" RGPD. Bien évidemment les progiciels type SIRH ou CRM sont directement impactés mais aussi, et nous allons nous focaliser dessus, les 2 applications les plus courantes, à savoir la messagerie et le serveur de fichiers.

Des systèmes qui ont atteint leurs limites

Côté messagerie, les mauvaises pratiques font que de nombreux

Coté serveur de fichiers, les droits d'accès ne sont pas forcément bien

Coté serveur de fichiers, les droits d'accès ne sont pas forcément bien gérés (ou maintenus), pouvant aboutir sur l'accès à des données personnelles (ex : bulletin de Salaire) par des personnes non-autorisées

acteurs internes à l'organisation). De plus la piste d'audit n'est pas toujours activée, de même la gestion des versions.

Au sens RGPD, l'organisation est responsable dans le cas où un bulletin de salaire, un contrat, un entretien d'évaluation, un bon de commande/facture

des moyens inavouables, qu'il soit stocké sur un serveur de fichier ou transmis par email. Inutile de souligner que cela va mettre sous contrainte très forte les organisations et imposer des changements dans les pratiques.

Les organisations vont donc devoir bannir l'utilisation de l'email et du serveur de fichiers pour toutes les informations personnelles. Nous

Les organisations vont donc devoir bannir l'utilisation de l'email et du service de fichiers pour toutes les informations personnelles. Nous rajouterons de retenir ce concept aussi pour les contenus sensibles. Cela permet de s'appuyer sur la contrainte du RGPD pour augmenter significativement le niveau de sécurité alors que le nombre d'attaques explose, que ce soit à des fins criminelles (ransomware, etc.) ou d'espionnage (21 % du vol de données est concentré sur le secteur industriel, les activités gouvernementales, l'activité de conseil et la recherche).

Quelles solutions pertinentes envisager ?

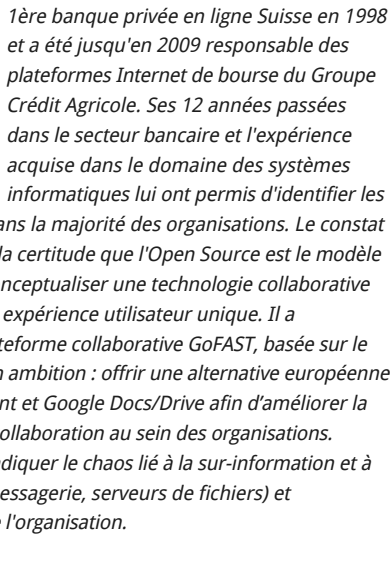
Les meilleures pratiques vont désormais s'appuyer sur les plateformes de travail collaboratif et de GED. A l'heure où le Digital Workplace et la GED

- de centraliser tout le contenu dans l'entrepôt **GoFAST** pour limiter les risques de fuites de données sensibles en bannissant le stockage des

- documents dans les messageries, les supports amovibles, PC personnels, etc.
- de gérer simplement les accès, permettant aux utilisateurs de facilement comprendre qui a accès à quels documents.
- de séparer les droits dits « métier » de l'administration technique et éviter l'effet « Snowden » (le superadministrateur n'a pas accès par défaut au documents).
- de suivre les créations des documents et les mises-à-jour des versions (piste d'audit associée : qui a ajouté ou modifié le document et quand).
- de catégoriser les documents ayant des données sensibles ou personnelles et de les rassembler dans des espaces dédiés avec uniquement des membres habilités.
- d'envoyer un lien de téléchargement pour les contenus sensibles utilisant un canal sécurisé et auditable.
- de publier les fiches de paie (ou tout autre contenu personnel) dans les espaces privés des collaborateurs.
- les fichiers supprimés restent récupérables durant une période donnée.

dont le respect de normes comme ISO9001, amélioration de la productivité et de la collaboration.

Christophe Potter



Sur le même sujet:



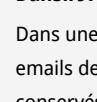
Je m'inscris

 1 commentaire

Conformité Dématérialisation Collaboration

Connectez-vous ou inscrivez-vous pour publier un commentaire

A LIRE SUR ARCHIMAG >

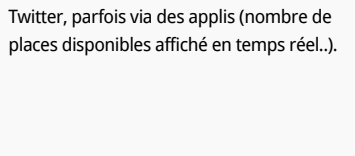


Dans une

conservés pendant des années, souvent sans limite de temps. Si une partie des éléments d'une signature, tels que nom, prénom, adresse mail professionnelle, sont considérés comme des données personnelles et que le droit à l'oubli, par exemple, s'y applique, il me semble assez complexe de nettoyer des boîtes de messagerie, en particulier pour les emails multi-destinataires ou il serait nécessaire de supprimer un destinataire sans supprimer l'email tout entier. Est-ce que le RGPD nous oblige à répondre à cette problématique ?

mai 16, 20

1



archimag guide pratique Pint

