IRON MOUNTAIN®

POURQUOI LE RGPD EST L'OPPORTUNITÉ DE METTRE EN PLACE UNE VRAIE GOUVERNANCE DE L'INFORMATION

PAR MARLÈNE CAILLEAU

Les organisations sont encore nombreuses à exposer (laisser en accès libre en interne) leurs données sensibles (informations personnelles, données de santé, bancaires, identités, etc.). Et ce, alors que le RGPD fait foi depuis mai 2018, que les cybermenaces sont en constante augmentation et que la Cnil a annoncé que le temps de la tolérance touchait à sa fin et qu'elle allait désormais se montrer beaucoup plus stricte vis-à-vis des organisations qui tardent à se mettre en conformité.

Dans une récente étude, Varonis* rappelle justement qu'en moyenne, 22% des fichiers d'une organisation sont accessibles à l'ensemble des collaborateurs, et que dans plus de la moitié des entreprises, ce sont au moins 1 000 fichiers contenant des données sensibles qui sont laissés en accès libre à tous les collaborateurs.

CONTRÔLE ET DESTRUCTION OBLIGATOIRES

L'absence de contrôle et de purge exposent clairement ces fichiers sensibles. Toujours selon cette même étude, 87 % des organisations auraient même plus de 1 000 dossiers contenant des données sensibles dont elles n'ont plus l'utilité et 40 % compteraient plus de 1 000 utilisateurs autorisés à accéder au réseau, mais inactifs. Les habitudes en matière de protection des informations sensibles doivent donc changer. Et pour cela une prise de conscience est nécessaire. À moins qu'il ne faille un contrôle et une amende pour qu'enfin certaines organisations ne s'emparent du problème.

DES PLAINTES EN HAUSSE

Depuis mai 2018, les organisations sont pourtant sensibilisées à la protection des données à caractère personnel. D'ailleurs, la Cnil dans son rapport annuel indique que les plaintes qu'on lui a adressées ont considérablement augmenté (11 077 au total, +32% par rapport à 2017), tout comme les demandes d'information. Ces plaintes portent principalement sur la diffusion des données sur Internet et concernent le secteur marketing/commerce notamment la prospection par SMS et la publicité par e-mail. Non seulement les professionnels ont pris conscience de leurs obligations, mais surtout les particuliers ont exercé leurs droits.

TRIPLE EFFET

Le RGPD est entré en vigueur 2018, à un moment où l'on assistait de manière concomitante à la montée en puissance de l'automatisation au sein des organisations (robotisation, processus dématérialisée et en temps réel, etc.), à la croissance du volume des données (liée à l'essor de la mobilité et de l'accès instantané à l'information) et à l'importance prise par la confidentialité de ces mêmes données (cybercriminalité oblige). Ce nouvel environnement impose une adaptation de la gestion de l'information.

CHANGEMENT DE PARADIGME

D'autant que les méthodes de travail aussi évoluent. Aujourd'hui, les organisations se recentrent sur leur cœur de métier. Elles ont de moins en moins de scrupules à externaliser toutes les opérations qui ne sont pas stratégiques et à **automatiser certains processus métiers** pour gagner en agilité et faciliter les prises de décision. Mais pour cela, il convient de définir et d'appliquer une politique de gouvernance globale. D'où l'importance de cartographier et de maîtriser les informations qui circulent dans l'organisation et de tout mettre en œuvre pour les protéger, limiter leur exposition et éviter les failles de sécurité.

LE RGPD : UNE OPPORTUNITÉ POUR MIEUX GÉRER LE CYCLE DE VIE DES DOCUMENTS

Le RGPD peut donc être vu comme une opportunité. C'est d'ailleurs la recommandation d'Iron Mountain à ses clients, l'idée étant de s'appuyer sur ce règlement pour pousser les entreprises, dès l'intégration d'un document (ou dès sa réception, s'il n'est pas produit en interne), à associer à ce document **une durée de vie** et ensuite à l'éliminer pour ne pas que les serveurs soient submergés d'informations et de documents que l'entreprise ne serait plus dans l'obligation de conserver (voire, l'obligation de détruire).

L'E-MAIL, UN SUJET DE PLUS EN PLUS DIFFICILE À MAÎTRISER

L'e-mail est justement dans le collimateur de cette nouvelle gestion de l'information et pose un vrai problème de maîtrise. D'une part, parce que les utilisateurs font face à un immense vrac numérique, et d'autre part, parce qu'ils ne maîtrisent pas les données incluses dans ces e-mails qui circulent à une vitesse vertigineuse. Les e-mails sont donc le plus souvent mal référencés, alors qu'ils exigent une analyse de chaque document et d'être rattachés à un dossier. Ils sont finalement mis de côté, mais conservés malgré tout et ce, alors qu'ils sont susceptibles de contenir énormément de données personnelles. Dans les organisations françaises, dans le doute on s'abstient et **on conserve tout**. Et c'est là, le problème.

DE L'EAU AU MOULIN DES ARCHIVISTES

Il est important de comprendre qu'à partir du moment où l'on dispose d'un environnement, d'un logiciel, d'une solution ou d'une application qui embarque de la donnée personnelle, on est concerné par le RGPD. Sans compter qu'il n'y a pas que le RGPD qui fait foi. Derrière lui, il y a aussi la loi française, les lois européennes, les lois propres à chaque pays et tout un environnement réglementaire (par exemple le code des assurances) qui reste applicables. En échangeant avec Sonia Lieutier, responsable Documentation & Veille juridique chez Gecina, elle a confirmé que "Le RGPD n'est donc pas le seul dogme. Il ne fait d'ailleurs que s'appuyer la démarche initiée depuis longtemps par les archivistes, mais a largement contribué à la légitimer auprès des directions et des collaborateurs pour les sensibiliser aux documents (et aux données) qu'ils manipulent ".

RAPPEL DES OBLIGATIONS

Le RGPD rend obligatoire, dans certains cas, la désignation d'un **DPO** qui peut être interne ou externe. La présence d'un "gardien du temple" est nécessaire pour répondre à toutes les questions de mise en conformité et de privacy-by-design par exemple. Il y a ensuite l'obligation de documenter procédures et liens contractuels, mais aussi de sécuriser la partie hébergement des données, d'être plus transparent à son sujet et de cartographier les données. Sachez également que dès que des données sortent du territoire européen, l'organisation est dans l'obligation de le déclarer. L'objectif étant, ensuite, de mettre tous les pare-feux autour de ces données pour sécuriser les flux.

PAS DE PRIVÉE SANS SÉCURITÉ

Je ne peux qu'insister sur le fait que, dès qu'une organisation collecte une donnée sur la vie privée d'une personne, que ce soit ses données de santé, ses données bancaires ou autres, elle entre dans le cadre du RGPD. L'organisation est du moins tenue de préserver la confidentialité de ces données. Or, il lui est impossible de sécuriser ces données si elle ne sait pas où elles sont. Sans maîtrise de la localisation, des lieux, des systèmes d'hébergement et des applicatifs (s'ils sont multiples), impossible d'assurer cette sécurité.

> DEPUIS MAI 2018, LES ORGANISATIONS SONT POURTANT SENSIBILISÉES À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL. D'AILLEURS, LA CNIL DANS SON RAPPORT ANNUEL INDIQUE QUE LES PLAINTES QU'ON LUI A ADRESSÉES ONT CONSIDÉRABLEMENT AUGMENTÉ (11 077 AU TOTAL, +32% PAR RAPPORT À 2017)

LA SÉCURITÉ : L'AFFAIRE DE TOUS

La sécurité est par ailleurs l'affaire de tous.
L'IT aura beau développer tous les pare-feux nécessaires au maintien de cette sécurité, mettre hors ligne un certain nombre d'informations, si l'individu, au quotidien, n'est pas le relais de cette confidentialité et de cette sécurité, forcément il y aura des trous dans la raquette. Il ne faut donc pas attendre de l'IT qu'il ait la solution miracle. En revanche, il peut mettre certains outils à disposition. La sécurité des données passe donc par une cartographie complète, la rédaction de procédures et un audit en temps réel : "Je dis ce que je fais, je fais ce que je dis, et je contrôle que j'ai fait et ce que j'ai dit". C'est du bon sens.

FAUT-IL AVOIR PEUR DES SANCTIONS ?

Malgré l'ampleur des sanctions prévues par le RGPD, il ne faut pas perdre de vue que l'autorité de contrôle est parfaitement consciente qu'une partie des données personnelles a été créée, reçue ou collectée dans un contexte "hors RGPD". Elle ne va donc pas avoir le même niveau de sanction avec un flux produit avant l'entrée en vigueur du règlement, et un flux produit après. Elle ne va pas non plus avoir le même niveau d'exigence avec une organisation dont la donnée personnelle est le cœur de métier et avec une organisation pour laquelle la donnée personnelle n'est pas une donnée vitale.

FAIRE PREUVE DE BONNE VOLONTÉ

Ce qui sera surtout vérifié, c'est la bonne volonté des organisations à se mettre en conformité, à partager le fait que la donnée personnelle est une donnée sensible et qu'un plan d'action a bien été instauré pour prendre en compte ces nouvelles exigences. Ensuite, certaines choses peuvent être résolues rapidement : un document à modifier, ajouter un avenant, etc. D'autres, en revanche, sont un peu plus complexes et nécessitent davantage de temps et/ou de moyens. Le plan de remédiation ne se fera donc pas du jour au lendemain et pourrait même s'étaler sur plusieurs années.

LES QUESTIONS POUR S'EMPARER DU SUJET

Oui, mais voilà, par où commencer ? Je préconise de catégoriser ainsi les questions qui se posent :

- les ressources : Qui s'occupe du sujet ? Qui nommer DPO ? Une externalisation est-elle possible ? La personne que j'ai en tête a-t-elle toutes les compétences nécessaires ? Nécessite-t-elle un accompagnement ?
- le terrain. De quoi exactement est composé mon fonds documentaire ? Comment puis-je montrer ce que j'ai déjà mis en œuvre ? Et prouver que je suis bel et bien en ordre de marche ?
- la stratégie. Que puis-je mettre en place ? Quelles procédures ? Comment responsabiliser les collaborateurs autour de ce que je veux créer et de ce à quoi j'ai pensé ? Comment puis-je m'assurer que tout cela est une réalité dans l'organisation et pas un simple postulat ? Si j'ai besoin de ressources supplémentaires, comment puis-je les chiffrer ?

Il n'y a pas de réponse toute faite. Cela dépend du contexte de chacun.

UNE CONSÉQUENCE POSITIVE

In fine, près d'un an après son entrée en vigueur, le RGPD n'est pas encore pleinement intégré ni compris. Mais il a certaines conséquences positives. Car pour protéger les données personnelles, les organisations doivent aujourd'hui intégrer que celles-ci ne leur appartiennent pas et les traiter comme un élément temporaire, qui leur aurait été confié, et non comme quelque chose dont elles sont propriétaires par défaut.

Les informations doivent donc être stockées avec un niveau de sécurité adéquat, pour que seules les personnes habilitées puissent y accéder. Ce changement de perception, aussi évident soit-il, est essentiel pour protéger les données personnelles.

Pour aller loin sur le sujet, visionnez **l'intégralité du webinaire sur le RGPD et la gouvernance de l'information organisé par Iron Mountain en cliquant ici.**

*2019 Global Data Risk Report

PARTAGEZ CE GUIDE:

NOUS PROTÉGEONS CE QUI A LE PLUS DE VALEUR POUR VOUS

0800 215 218 | IRONMOUNTAIN.FR

AU SUJET DE IRON MOUNTAIN

Iron Mountain Incorporated (NYSE : IRM) fournit des services de gestion de l'information qui permettent aux entreprises de réduire les coûts, les risques et les inefficacités de gestion de leurs données physiques et numériques. Fondée en 1951, Iron Mountain gère des milliards de ressources d'information, y compris des données de sauvegarde et d'archivage, des enregistrements électroniques, des numérisations de documents, des registres commerciaux, des destructions sécurisées et plus encore, pour des organisations à travers le monde entier. Visitez le site Internet de l'entreprise sur www.ironmountain.fr pour obtenir plus d'informations.

© 2019 Iron Mountain Incorporated – Tous droits réservés. Iron Mountain Incorporated et le symbole des montages sont des marques enregistrées pour Iron Mountain Incorporated.