IRON MOUNTAIN®

DESTRUCTION DES ACTIFS INFORMATIQUES : UN PASSAGE OBLIGÉ POUR LA CONFORMITÉ AVEC LE RGPD

Les sociétés qui manipulent les données personnelles de citoyens de l'Union européenne sont en pleine effervescence depuis l'entrée en vigueur du RGPD. Pourtant, malgré toute cette agitation, nombreuses sont celles qui passent à côté d'un élément crucial à propos de la fin du cycle de vie des données : la destruction des actifs informatiques, une composante pourtant incontournable de la démarche de conformité au RGPD.

Les sociétés qui conservent ou traitent les données personnelles de citoyens de l'Union européenne travaillent d'arrache-pied pour s'assurer de la conformité de leur entreprise au Règlement général sur la protection des données personnelles (RGPD) de l'Union européenne. Pourtant, en dépit de ces efforts, un grand nombre d'entre elles sont encore loin d'être conformes et cela malgré la mise en application de cette loi depuis le 25 mai 2018. En outre, beaucoup passent également à côté d'une exigence majeure du RGPD concernant l'autre extrémité du cycle de vie des données, à savoir le moment où il faut procéder à la destruction des actifs informatiques (DAI) concernés.

Ainsi, il est important de pouvoir prouver qu'on respecte le RGPD à la lettre grâce à la mise en œuvre d'une politique formelle de DAI, mais les entreprises négligent souvent cet aspect de la réglementation. Heureusement, il suffit de suivre quelques conseils avisés pour se doter sans trop de peine d'une politique de DAI.

LE RGPD, LA DAI ET LE RISQUE OMNIPRÉSENT DE VIOLATION DE DONNÉES

Les juristes de Lexology ont souligné les dispositions du RGPD qui attribuent aux contrôleurs des données et aux responsables de traitement des données un rôle plus étoffé. En matière de destruction des actifs informatiques, le recours à des fournisseurs externes (ainsi que tout autre fournisseur tiers concerné) relève désormais des prescriptions établies par le règlement européen au sujet des responsables de traitement des données.

D'après Brooks Hoffman, Directeur de la gestion des données chez Iron Mountain, les PDG des sociétés concernées par le RGPD sont particulièrement préoccupés par la nécessité d'éviter toute violation de données personnelles de citoyens de l'Union européenne.

« Le secteur de la DAI a un côté Far West. Sur le marché, il existe des sociétés qui ne font pas toujours les choses de la manière requise. Il est facile et tentant de réaliser des économies ici et là en appliquant le règlement à sa manière. Mais un tel choix », prévient-il, « risque de coûter cher plus tard. C'est même susceptible de générer des violations de données. »

SUR LA BRÈCHE : LES MESURES À PRENDRE EN MATIÈRE DE DAI

La destruction des actifs informatiques concerne notamment le sort qui est réservé à un certain nombre d'équipements (PC, smartphones, serveurs, disques durs...) en fin de vie, sur lesquels des données personnelles de citoyens de l'UE sont susceptibles de subsister. C'est exactement le cas où il est impératif de disposer à la fois d'une politique formelle de DAI définie par le contrôleur des données et d'un contrat formel qui lie le contrôleur des données à n'importe lequel de ses fournisseurs de DAI ou de traitement des données.

L'objectif est de décrire avec précision de quelle façon les données personnelles éventuellement présentes sur des équipements en fin de vie, destinés à être recyclés ou remis sur le marché, doivent être identifiées et effacées en toute sécurité. Il convient également de déterminer clairement les rôles et de définir les procédures à suivre tout au long de la chaîne de contrôle pour tout ce qui concerne le processus de destruction des actifs informatiques.

Il est en outre nécessaire de définir formellement, en collaboration avec le contrôleur des données et les responsables de traitements des données, les procédures de notification à suivre en cas de violation de données. Les plans de prévention contre les violations de données préparés par les responsables de traitement des données devraient être couchés par écrit, de même que les processus d'action postérieurs à une violation de données et tout engagement financier pris, le cas échéant, par le contrôleur des données à titre de réparation.

«Si vous envisagez de faire appel à un partenaire externe pour votre DAI, il convient bien entendu de le prévenir que vous allez émettre une notification de violation de données dans un délai de 72 heures après les faits et engager des crédits de façon contrôlée », explique Hoffman Brooks. « Mais il faut aussi veiller à ce que ce soit au fournisseur d'assurer la gestion financière de la notification d'une violation de données spécifique et des mesures à prendre postérieurement.»

En l'espèce, d'après Hoffman Brooks, il peut se révéler très utile de veiller à ce que le fournisseur de DAI dispose de capitaux suffisants, qu'il jouisse d'une bonne réputation dans le secteur et qu'il justifie d'une certification remise par une tierce partie agréée. En cas de violation de données potentielle, il faut rechercher spécifiquement des fournisseurs qui sont correctement assurés contre les erreurs et omissions, ou assurance de cyber-responsabilité.

Le profil du fournisseur de DAI idéal comporte encore d'autres caractéristiques, qui doivent également figurer dans votre politique de DAI. Voici un article de référence qui couvre certaines d'entre elles. Il est intéressant de noter qu'un questionnaire destiné aux fournisseurs services de traitement de données, développé dans les îles Anglo-Normandes, peut contribuer à étoffer d'autres politiques d'entreprise concernées par le choix de ces fournisseurs, au-delà de votre politique de DAI et de la formalisation des documents contractuels visés par le RGPD.

> SEULES 19% DES ORGANISATIONS SONT CONFIANTES QUANT À LEUR CAPACITÉ À APPLIQUER LE «DROIT À L'OUBLI» DE LEURS CLIENTS, EN CONFORMITÉ AVEC LE RGPD DE L'UNION EUROPÉENNE.

POURQUOI FORMALISER VOTRE POLITIQUE DE DAI ?

Une entreprise a toujours intérêt à formaliser les bonnes pratiques qui président à son action et les politiques qui couvrent ses processus de stockage, de gestion et de destruction des données personnelles des citoyens de l'UE. Mais il est vrai que cela relève généralement davantage de la peur du gendarme que de la volonté de tirer les bénéfices d'une gestion vertueuse, tant les pénalités prévues en cas de non respect du RGPD sont importantes.

« Le RGPD constitue véritablement l'aboutissement d'une tendance générale en matière de confidentialité des données. Son caractère révolutionnaire pour le secteur réside dans le fait qu'il accorde aux individus des droits très puissants, comme celui de refuser le suivi et le stockage de leurs données personnelles par des sociétés. Les enjeux sont dès lors très élevés, car les amendes pour non-conformité au RGPD sont astronomiques », estime Hoffman Brooks. « Il est donc plus important que jamais de disposer d'une politique de DAI formalisée et exhaustive, en particulier pour les grandes sociétés, où il est possible que chaque entité ait des pratiques légèrement différentes dans ce domaine. Lorsque 75 % des entités d'une entreprise ont une pratique correcte de la DAI, cela signifie que 25 % ont une pratique incorrecte. C'est un problème. »

WE PROTECT WHAT YOU VALUE MOST

0800 215 218 | IRONMOUNTAIN.FR

À PROPOS D'IRON MOUNTAIN

Iron Mountain Incorporated (NYSE : IRM) offre des services de gestion de l'information qui permettent aux entreprises de baisser leurs coûts, de limiter leur exposition aux risques et d'éliminer les inefficacités en matière de gestion des données numérisées et sur support physique. Fondée en 1951, la société Iron Mountain prend en charge pour les entreprises du monde entier la gestion de milliards d'informations quel que soit leur support, tels que données de sauvegarde et d'archives, documents électroniques, imagerie documentaire, documents professionnels et destruction sécurisée. Pour plus d'informations, visitez le site Web de la société à l'adresse www.ironmountain.fr.

FRDM-ART-022119A