Conformité RGPD : de nombreuses entreprises à la traîne

Le 25 mai 2018, le Règlement Général sur la Protection des Données (RGPD) entrait en vigueur. Deux ans après, de nombreuses entreprises ne sont toujours pas en conformité avec ce règlement qui ne peut se résumer à une liste précise d'actions à mettre en œuvre et de cases à cocher. Les risques en cas de non-conformité sont pourtant très importants tant au niveau de la réputation de l'entreprise qu'au niveau financier : les amendes pouvant s'élever jusqu'à 20 millions ou jusqu'4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Un règlement européen

Le RGPD remplace une directive qui datait de 1995. Depuis lors, le monde a bien évolué, la digitalisation étant passée par là et l'exploitation abusive de nos données personnelles ne faisant que commencer. La Commission Européenne a dès lors entrepris de réformer profondément la directive en la remplaçant par un règlement avec un double objectif :
1.Renforcer la protection des données personnelles des citoyens européens ;
2. Clarifier l'environnement réglementaire des entreprises par une uniformisation au niveau européen.

Le RGPD offre ainsi un cadre réglementaire adapté à la réalité du monde numérique actuel, tout en donnant au citoyen le contrôle de ses données personnelles.

Pourquoi tant d'acteurs en non-conformité ?

Tout d'abord, certaines entreprises pensent ne pas être concernées par le RGPD. Or toute entreprise située sur le territoire européen et ayant des parties prenantes - personnel, investisseurs, clients, fournisseurs ou même prospects ou encore partenaires - est concernée par le RGPD.

Deuxièmement, le Règlement prévoit un principe de responsabilisation des entreprises. Les organisations sont censées de facto avoir fait le nécessaire pour protéger les données personnelles des citoyens et être en mesure d'en apporter la preuve. Dès lors, on ne peut pas dire «je ne savais pas». Les entreprises ne peuvent se permettre d'attendre un contrôle pour réagir et se mettre en ordre de marche.

Aussi, la mise en conformité est complexe en ce sens qu'elle concerne tous les pans de l'entreprise et ne peut se réduire à une liste de choses à faire ou à la mise en place d'une solution «one size fits all». Elle ne se limite pas non plus au département juridique ou IT, puisque 80% de la mise en conformité est de nature organisationnelle. Il ne s'agit donc pas d'adresser des points isolés çà et là mais de repenser l'organisation voire la culture d'entreprise. Enfin, nombreux sont ceux qui pensent que le consentement est la seule base légale à l'exploitation de données personnelles. Certains acteurs renoncent à se lancer dans l'entreprise délicate de l'obtention de tels consentements. Pourtant, comme nous l'avons évoqué, les risques en cas de non-conformité peuvent être conséquents.

Base légale : il n'y a pas que le consentement !

En vertu du RGPD, les entreprises doivent avoir une base légale pour traiter des données personnelles. On entend souvent parler du «consentement». Il est important toutefois de noter que d'autres bases légales existent. Ainsi il est permis d'utiliser des données personnelles sans consentement si ces dernières sont nécessaires à l'exécution d'un contrat, si leur utilisation répond à une obligation légale, ou si leur possession représente un intérêt vital ou encore pour l'intérêt légitime de l'entreprise. Dans ce dernier cas, il conviendra de mettre «en balance» les droits des personnes concernées et l'intérêt légitime de l'entreprise. Cet intérêt légitime ne peut donc être considéré comme une base légale «par défaut» de la part de l'organisme. Par ailleurs, le fait que le consentement soit la base légale dont on parle le plus ne signifie en aucun cas qu'elle soit plus importante aux yeux du RGPD et du législateur. Il convient juste de définir la base juridique la plus appropriée pour les activités de traitement des données à caractère personnel.

Sous la pression des partenaires économiques

Si le RGPD a pour objet de protéger les données personnelles des différentes parties prenantes : employés, clients, fournisseurs, etc., la pression pour la mise en conformité vient également de la part des organisations avec lesquelles les données personnelles sont partagées. Ainsi, ce sont les différents acteurs de la chaîne de valeur qui exigent que leurs partenaires de cette même chaîne soient en mesure de démontrer un niveau suffisant de conformité au RGPD. En outre, le niveau de conformité est devenu une considération de plus en plus importante pour les investisseurs, les acteurs de Private Equity et autres sociétés qui acquièrent des entreprises.

Checklist RGPD ou mode d'emploi standardisé ?

Non, il n'existe rien de tel. En effet, la mise en conformité doit être fonction des risques, de l'environnement, des besoins et des ressources spécifiques à chaque entreprise.

Néanmoins le RGPD dessine un cadre incluant certains incontournables. A ce titre, on peut noter :
- la sensibilisation du personnel ;
- le mapping des données ;
- la mise en place et la revue de politiques dédiées ;
- la mise en place de procédures en cas de violation des données ou de requête d'utilisateurs ;
- la revue des contrats avec les sous-traitants et les partenaires ;
- la sécurité IT ;
- la mise en place d'un registre des traitements.

Enfin, le plan de mise en conformité doit couvrir par ordre de priorité les risques les plus importants pour les données personnelles des citoyens. Et ces risques varient selon la nature de l'activité de chaque entreprise.

La mise en conformité, un exercice continu

Les défis en matière de protection des données à caractère personnel vont sans nul doute évoluer dans une danse en trio avec les amendements du Règlement et les changements de jurisprudence, le tout dans le souci de s'adapter à la réalité numérique. Par ailleurs, les nouveaux employés doivent également être formés au RGPD. L'exercice de conformité revêt donc un caractère permanent. Ainsi, dans un écosystème digital en perpétuelle évolution, l'adaptation continue des acteurs est une évidence.

Tout bénéfice

Bien que la mise en conformité ne soit pas une promenade de santé, il ne s'agit pas d'un exercice insurmontable. L'accompagnement par des experts privilégiant une approche pragmatique visant une mise en conformité rapide et efficace, et amenant la sécurité des données personnelles au niveau adéquat est parfois nécessaire. L'objectif visé doit être d'appréhender le RGPD non comme un fardeau ou une épée de Damoclès, mais comme une opportunité d'amélioration des organisations, des opérations et de la sécurité informatique.

Laurence PONCHAUT, Head of GDPR services
Cyril CAYEZ, co-Founding Partner
HACA Partners
http://www.hacapartners.lu/

L'autre virus

Par Olivier de BERRANGER, directeur général délégué en charge de la gestion d'actifs, La Financière de l'Echiquier

Dans l'après-midi du 27 juin 2017, on apprenait qu'un virus menait une vaste attaque contre un grand nombre de sites internet et de systèmes d'information, notamment en Europe.

Si la facture d'une attaque est toujours délicate à estimer, le ransomware[1] NotPetya aurait fini par coûter près de 10 milliards de dollars selon diverses estimations. Au moins 2 000 entreprises visées, dont la SNCF, WPP ou encore le laboratoire pharmaceutique MERCK. SAINT-GOBAIN reconnaîtra ainsi près de 250 millions d'euros de perte de chiffre d'affaires et 80 millions de résultat d'exploitation évaporés. Plus récemment, le point commun entre des entités bien différentes comme le Parlement norvégien, l'usine Tesla au Nevada ou la sécurité sociale italienne est d'avoir été la cible de cyberattaques sophistiquées.

Dans le cyberespace, la lutte mondiale pour le contrôle de l'or noir de l'économie numérique, la data, bat son plein avec une large palette d'offensives, du phishing ou hameçonnage de données personnelles aux ransomwares. Des attaques qui se sont intensifiées cette année, celles ciblant les banques auraient ainsi triplé pendant le confinement selon l'agence Moody's. Même le secteur de la santé n'est pas épargné, et la Croix-Rouge a connu les attaques les plus virulentes de son histoire en mars dernier.

Un marché en plein effervescence

Enjeu stratégique pour les entreprises depuis l'accélération de leur digitalisation et la généralisation du télétravail confirmée par la crise du coronavirus, la sécurité numérique est aujourd'hui un marché en pleine effervescence, évalué à 43 trillions de dollars[2]. Satya Nadella, directeur général de MICROSOFT, a estimé, fin avril, avoir vu s'opérer deux ans de transformation digitale en l'espace de deux mois... Cet emballement inédit a généré naturellement une forte hausse de la demande de solutions de sécurité.

Nombre d'entreprises dans le monde ont déjà augmenté leurs investissements pour améliorer leur hygiène cybernétique, leurs capacités de prévention, leurs protocoles de détection ou encore de réaction.

Les dépenses mondiales en logiciels et services de sécurité numérique devraient atteindre 125 milliards de dollars en 2020 et augmenter de plus de 8% par an en moyenne pour peser plus de 170 milliards de dollars en 2024[3]. Une tendance structurelle forte que notre équipe de gestion a déjà identifiée, à l'image par exemple de nos investissements dans ZSCALER, leader de la cybersécurité cloud, ou dans OKTA, leader de la nouvelle architecture dite «Zero Trust Security».

Avec le changement climatique, le «cyber risque» est l'un risques majeurs identifiés par le Forum Mondial de Davos. Un risque contre lequel nombre d'entreprises doivent se vacciner et organiser leurs défenses. Et comme toujours, nouveaux risques signifient nouvelles opportunités. Bienvenue dans l'ère de la cyber-résilience

1) Logiciels malveillants prenant les données en otage
2) Cabinet d'analyse Canalys
3) Cabinet IDC

Conférences digitales :

Analyse du concept de « e-conferences parallèles »

L'agence de communication 360Crossmedia a organisé cette année la conférence annuelle de l'ATEL, avec une approche originale : speakers identiques, thèmes identiques, 2 expériences différentes. Un contenu fut ainsi dédié aux internautes et un autre réservé aux 40 personnes présentes physiquement. Analyse.

Le problème à résoudre

L'an passé, la conférence annuelle de l'ATEL a rassemblé 250 personnes. Après une première conférence en 2020 en mode 100% virtuel, le comité de l'association s'est retrouvé face à un dilemme : rester en mode 100% et risquer de décevoir des partenaires fidèles ou prendre le risque d'un événement physique. La solution trouvée en Août fut originale : d'une part, enregistrer dans un studio virtuel les présentations des speakers afin de livrer une conférence optimisée pour une diffusion sur internet; d'autre part, inviter 40 Trésoriers d'entreprises triés sur le volet – limite sanitaire oblige - pour assister à une présentation physique, dans un cadre extrêmement sécurisé au niveau du Covid19 : 20 chaises installées en cercle sur 2 rangs, 2 mètres d'écart partout, gants en latex pour les organisateurs, masque obligatoire pendant le networking et plateau repas servi sur des tables individuelles.

(left to right) Coralie BILLMANN, Head of PayPal Europe Treasury and Investments, Raphaela COVA de LIMA, Treasury Director, EMEA, Koch Industries et Winkie CHOI, Head of Amazon EMEA Treasury

Avantages et inconvénients

Une des grandes leçons de cette expérience, c'est qu'un speaker à l'aise depuis des années sur scène peut se retrouver tétanisé seul dans une pièce face à une caméra. Un autre enseignement, c'est que les internautes regardent beaucoup plus facilement une émission dédiée à un format digital, par comparaison avec le simple streaming d'un format physique. Les deux expériences débutèrent à la même heure. Et immédiatement, les avantages et les inconvénients firent leur apparition ! La conférence en ligne respecta un timing parfait, alors que la conférence physique accumula une série de petits retards.

Au niveau émotionnel, les 40 invités et les speakers ne cachaient pas leur joie : il s'agissait pour la plupart d'entre deux d'un premier événement physique depuis Mars. Beaucoup confièrent avoir été inquiets de venir, mais rassurés par l'application de règles très strictes. Le networking fut particulièrement qualitatif. Le contenu ne fut au final pas identique car si l'enregistrement en studio permet de suivre un script millimétré, une présentation physique suit un fil conducteur en laissant une large part à l'improvisation et aux interactions avec l'audience.

Le meilleur format

Tout le monde sort gagnant de cette nouvelle approche. Elle permet de redémarrer des événements physiques en minimisant les risques du fameux coup de téléphone qui annonce à tous les participants qu'ils doivent subir une quarantaine. D'autre part, l'enregistrement en studio permet aux speakers d'améliorer considérablement leur présentation en travaillant sur leur talent oratoire, leur contenu et en intégrant au montage des effets spéciaux.

Plusieurs speakers confièrent avoir beaucoup apprécié de pouvoir «répéter» leur présentation en studio avant de la livrer sur scène devant leur public. Un contenu créé spécifiquement pour internet peut également toucher une audience considérablement plus grande que celle d'un événement physique. Bref, ce type de format est appelé à se généraliser car le Covid19 a permis de booster considérablement les audiences digitales, tout en transformant le networking en produit de luxe. Le prochain défi consiste à offrir aux internautes une expérience de networking convaincante.