9 questions pour une approche pragmatique de la GDPR/RGPD

La nouvelle règlementation européenne en matière de protection des données entrera en vigueur en mai 2018. Plutôt que de se précipiter sur le déploiement de solutions techniques, il s'agit pour les entreprises d'approcher cette échéance de façon pragmatique en tenant compte du contexte et du risque particulier de l'entreprise et en s'appuyant sur l'existant.

LES AUTEURS

***Paul Barnabé**, Head of Market Industry, et **Flaviano Valvason**, Senior Manager expert en GDPR, tous deux chez Itecor.*

CONTACT

Ce n'est sans doute pas le premier article que vous rencontrez traitant de la nouvelle réglementation européenne en matière de protection des données – GDPR / RGPD pour faire court. Depuis quelques mois, la toile abonde en effet de nouvelles alarmistes sur les défis que représente la mise en conformité avec cette loi qui entrera en vigueur au le 25 Mai 2018. En résumé, la montre tourne et les entreprises ne seront pas prêtes.

Face à cette échéance, deux attitudes sont à éviter : ne rien faire parce que l'on ne se sent pas concerné (après tout, mon entreprise est en Suisse !) ou au contraire se précipiter sur un outil informatique ou dans un projet colossal de classification de toutes les données de l'organisation. Entre les deux, une approche pragmatique s'impose. Et pour commencer, éclaircissons quelques points…

1. Votre entreprise est-elle concernée ?

La GDPR/RGPD concerne toutes les entreprises ayant une orientation de marché européenne - autrement dit, qui ciblent des clients, résidents ou citoyens de l'UE. Pour les autres, la nouvelle réglementation européenne reste toutefois importante, car la prochaine Loi suisse sur la protection des données y ressemblera beaucoup, si l'on en croit le projet de révision adopté le 15 septembre par le Conseil fédéral. Pour une grande majorité des organisations suisses, il va donc falloir se conformer au nouveau cadre européen.

2. Qu'est-ce qui change ?

Principal changement, la nouvelle règlementation étend la notion de responsabilité de l'entreprise quant aux données personnelles qu'elle traite- on parle de Responsabilité de bout-en-bout (tout au long du cycle de vie des données personnelles). A titre d'exemple, une organisation employant une solution en ligne (fournisseur de type SaaS) pour envoyer une newsletter à ses clients, devra désormais se soucier de la manière dont les données sont protégées et traitées par le fournisseur cloud. Plus question de se défausser sur un prestataire de service en cas de violation de la loi…

3. Quelles fonctions de l'entreprise sont impactées ?

Les changements à venir concernent bien sûr l'IT, la sécurité des données et la gouvernance. Mais pas seulement ! Le marketing qui propose un formulaire de contact en ligne sans signaler ce qui sera fait des données, est tout autant concerné. Idem pour le service client, les ressources humaines ou le service archivage : tous sont susceptibles d'être impactés dès lors qu'ils participent au traitement de données personnelles. Sans oublier le département communication chargé de préparer la diffusion d'informations relatives à des brèches / violations éventuelles. D'où l'importance de confier les initiatives de mise en conformité à des équipes mixtes à même de développer une vue à 360° des traitements de données personnelles opérés dans l'entreprise.

4. Sur quelles bases s'appuyer ?

Heureusement, face au défi de la GDPR / RGPD, les entreprises ne partent pas de zéro. Elles sont déjà en conformités avec toute une série de lois locales, mêmes si ces lois ne prennent pas toutes en compte les aspects relatifs aux données personnelles. Dans bien des cas, elles ont également mis en œuvre des contrôles internes et déployé des outils de mesure des risques et de gouvernance ou de sécurité de type ISO (ISO 27000, 27005/31000, 27018) sur lesquels s'appuyer. Sans compter les organisations de certains secteurs – finance, santé – qui sont déjà soumises à des règlementations spécifiques couvrant en partie certains aspects de la GDPR / RGPD.

5. De combien de temps dispose-t-on ?

Il faut agir vite, mais il n'y a pas lieu de se précipiter : la GDPR / RGPD entre en vigueur en mai 2018 et le régulateur ne s'attend sans doute pas à ce que les entreprises soient 100% prêtes à cette date. Il importe en revanche que les organisations disposent à cette échéance d'une idée claire de l'écart qu'elles ont à combler et d'une roadmap solide des mesures mises en œuvre ou planifiées.

6. Par quoi commencer ?

Une démarche pragmatique commence par une cartographie de la situation actuelle de l'entreprise en matière de données personnelles et par une compréhension de son contexte particulier : L'entreprise gère-t-elle des données personnelles ? Quelles catégories (classification) ? De quels traitements ces données font–elles l'objet ? Quelles fonctions de l'entreprise sont en charge de ces traitements ? Quels sont les flux de données ? Qui a accès à quelles données et pourquoi ?

Mais aussi par un état des lieux de ce qui est déjà fait : Quelles mesures de gouvernance, de contrôle interne sont déjà en place ? Quels outils et techniques de protection sont déjà déployés ?
Cette compréhension de l'existant permet de faire une évaluation du risque spécifique à l'entreprise par rapport aux exigences de la nouvelle règlementation. C'est seulement cette analyse – couplée si nécessaire à une analyse de risques détaillées (Data Protection Impact Assessment) - qui permet de décider de façon pragmatique des mesures à mettre en œuvre (sur les aspects légaux, techniques et organisationnels) et de considérer d'éventuels outils ou processus à déployer.

7. Quel impact sur la gouvernance ?

La nouvelle réglementation européenne rend les entreprises responsables de l'intégralité du cycle de vie des données personnelles qu'elles détiennent. Dès la collecte, le client-utilisateur doit donner son consentement sur ce qui sera fait de ses données personnelles. Et il doit ensuite pouvoir les modifier, voir retirer son consentement et en cas de violation de la loi, pourrait exiger la suppression de ses données personnelles. Il faut aussi informer l'utilisateur en cas de transfert ou si une brèche ou violation menace de mettre ses données entre les mains de tiers. Tout au long du cycle de vie de la donnée, l'entreprise doit s'assurer que ses traitements sont légaux et respectent les principes de base de la loi – pas question par exemple de collecter des données qui ne seraient pas nécessaires aux traitements annoncés pour en disposer « en cas de besoin ». Il s'agit d'autre part d'intégrer la protection des données personnelles dès le début des projets (privacy-by-design), par exemple au moment de la conception d'un formulaire d'inscription à un événement, ou lors de la définition des fonctionnalités d'un objet connecté. Au-delà d'un renforcement de la gouvernance, il s'agit d'un changement profond des manières de faire qui nécessite l'attention - si ce n'est la formation - de tous les collaborateurs. Les données personnelles des clients sont un bien précieux et c'est de la responsabilité de tout à chacun, au sein de l'entreprise, de les protéger et de les exploiter avec discernement !

Tout le cycle de la donnée doit être legal.

8. Quels nouveaux rôles ?

Outre les changements de procédures, de contrôles et de policies, la GDPR/RGPD introduit de nouveaux rôles dans l'entreprise.

A commencer par le Data Protection Officer, un profil hybride (juridique, sécurité) chargé de superviser les pratiques de l'entreprise en matière de protection des données et
de s'assurer qu'elles respectent les droits des individus (renseignement, rectification, etc.). C'est à lui que s'adresseront par exemple des clients désirant savoir connaître quelles données sont collectées, pourquoi, comment, comment solliciter une rectification, etc. C'est aussi l'interlocuteur privilégié avec les préposés (confédération, cantons).
Deuxième fonction tout aussi importante, le « responsable des traitements » proche des métiers et qui définit la finalité et les moyens mis en œuvre pour le traitement des données Un troisième rôle étant le sous-traitant qui traite les données pour le compte du responsable de traitement.

9. Quel impact sur la sécurité informatique ?

Bien que l'informatique ne soit pas la seule fonction impactée par le nouveau cadre, la mise en conformité de l'entreprise débouchera souvent sur le déploiement ou le renforcement de solutions IT. Les domaines suivants du SI sont concernés :

Contrats avec les fournisseurs Cloud. L'entreprise est responsable des données personnelles, y compris lorsqu'elles sont stockées ou traitées par un prestataire tiers, et notamment un service cloud IaaS, PaaS ou SaaS (Office 365, Salesforce, Workday, etc.). Pour faire court, les serveurs ne sont plus là, mais la responsabilité reste et les contrats doivent être réévalués. Où les données sont-elles stockées ? Comment sont-elles protégées ? Qui y a accès ? Est-il possible de les modifier et de les effacer si le client final en fait la demande ? Le SLA prévoit-il une notification de l'entreprise en cas d'incident de sécurité ?

Identity Access Management. Difficile de remplir les exigences de la GDPR / RGPD si l'on ne sait pas qui dans l'organisation a accès à quelles données et qui en est responsable. Une stratégie IAM performante permet aussi d'identifier rapidement si les données d'un client ont été compromises.

Anonymisation & chiffrement. En dépit des multiples outils mis en place pour protéger les systèmes de l'entreprise, il arrive que des données personnelles soient dérobées. L'anonymisation et le chiffrement des données réduisent l'impact de tels incidents.

Master Data Management. Lorsqu'un client demande la rectification de l'une de ses données personnelles, l'exercice peut devenir très compliqué si - comme c'est souvent le cas – cette donnée se trouve dans de multiples systèmes (CRM, outil de comptabilité, etc.). L'opération est bien plus aisée si tous les systèmes obéissent à un référentiel maître. La conformité avec la GDPR / RGPD est ainsi l'occasion de ressortir le projet MDM du tiroir, avec de multiples autres bénéfices à la clé.