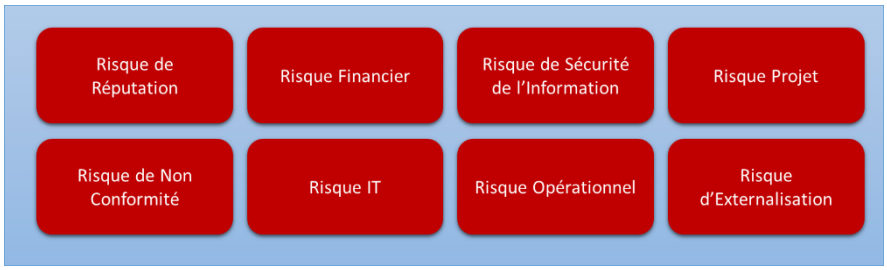
RGPD : RISQUES OU OPPORTUNITÉS ?

L'exigence de conformité au Règlement Général sur la Protection des Données personnelles (RGPD) est maintenant dans tous les agendas des directions générales, juridiques, risques, IT et métiers. La conformité au règlement doit être en conséquence intégrée dans le portefeuille de projets et du cycle budgétaire de la rentrée pour ceux qui ont pris de l'avance et dans le suivant pour ceux qui sont déjà en retard. Il n'y aura pas d'autres alternatives avant mai 2018.

Après cette période anxiogène de l'annonce de ce nouveau règlement, les entreprises les plus matures ont enfin compris les enjeux de conformité non seulement juridiques, métiers mais aussi IT. Certaines d'entre elles ont pris de l'avance et enclenché la nécessaire phase de pilotage et de coordination de leur projet RGPD intégrant un DPO ou non. Pour cela, il leur faut assurer la mise en place progressive de la conformité et garantir ainsi au législateur leur bonne foi quant à la maitrise de leur risque de non-conformité règlementaire à partir de mai 2018. Cette gestion du risque peut aussi laisser place à des opportunités majeures et structurantes pour les organisations grâce à de nombreuses exigences que la nouvelle réglementation impose. En voici un florilège qui permettra de considérer ce règlement pour certains comme un verre à moitié vide et pour d'autres comme un verre à moitié plein. Il est acquis que ces derniers auront un net avantage sur les autres …

Approche risques

Les risques liés au règlement sont connus de tous. Il est quand même de bon ton de se les lister car ils impactent non seulement les Systèmes d'Information mais aussi l'organisation tout entière :



- **Risque de Réputation** : la notoriété de l'entreprise quant à sa capacité de garantir une protection durable de ses données personnelles vis-à-vis de ses clients et de ses salariés. Une défaillance, une violation de données personnelles et c'est l'entreprise toute entière qui est mise à mal.
- **Risque de Non-Conformité :** la non-conformité est un risque majeur pour les organisations. Elle est avant tout règlementaire, juridique et contractuelle.
- **Risque Financier :** les sanctions financières sont extrêmement lourdes et inédites : 4% du CA globale de l'entreprise ou 20 M€ ! Il est donc majeur quelle que soit la taille de l'organisation.
- **Risque IT :** les risques liés aux SI sont nombreux car l'IT est fortement impacté à travers le RGPD : la gouvernance, les cartographies, les processus, la technologie, les ressources, …
- **Risque de Sécurité :** la sécurité informatique est au cœur du dispositif et le RSSI est fortement impliqué dans le respect lié à la sécurité de l'information : confidentialité, intégrité et disponibilité. Un processus dédié autour de la violation de données personnelles doit aussi être mis en place rapidement.
- **Risque Opérationnel :** l'absence de processus clés respectant un grand nombre d'exigences notamment autour des notions d'Accountability et de Consentement représente aussi une sérieuse menace.
- **Risques Projets :** ne pas respecter l'exigence de Privacy by Design ou by Default peut conduire à des projets à être déclarés non conformes en termes de protection des données personnelles résultant des futures applications mises en production.
- **Risques d'Externalisation** : la sous-traitance IT est aujourd'hui omniprésente dans toute organisation. Elle représente une menace supplémentaire car le sous-traitant doit lui aussi respecter les mêmes exigences en termes de réglementation et se retrouve sous l'autorité et la responsabilité de l'entreprise cliente.

Ces risques existent et doivent être identifiés, traités, gérés et intégrés dans le référentiel de risques de l'entreprise. Ils sont aussi et heureusement porteur d'espoirs car le risque peut être aussi traité comme une opportunité.

RGPD : RISQUES OU OPPORTUNITÉS ?

Approche opportunités

Il est important dans cette démarche de transformer, dans la mesure du possible, le risque en opportunité si ce premier a été identifié et maîtrisé. En effet cela est possible à partir d'une analyse fine à la fois sur le traitement à long terme des risques identifiés mais aussi sur certaines exigences impactant fortement l'organisation et certains de ses processus notamment ceux liés à l'IT. En voici quelques-unes avec leur début de réponse :

- **Opportunité d'Image** : une organisation qui collabore sereinement avec le régulateur et qui communique auprès de ses clients le respect de sa conformité réglementaire véhicule une image positive vis-à-vis de ses actionnaires, collaborateurs et futures recrues.
- **Opportunité de Gouvernance des données** : les exigences réglementaires en matière de données personnelles permettent l'implémentation durable de bonnes pratiques en matière de gouvernance de l'information. Notamment avec la nomination d'un DPO garant de la conformité RGPD associée à une cartographie rigoureuse et la tenue d'un registre de traitement de l'ensemble des données de l'entreprise.
- **Opportunité Business :** l'entreprise qui garantira sa conformité au règlement pourra être éligible à certains appels d'offre l'exigeant. Elle sera aussi identifiée prioritairement dans certaines circonstances en tant que sous-traitant vis-à-vis d'autres concurrents moins scrupuleux.
- **Opportunité de Proximité avec les Métiers :** une occasion unique de rapprocher l'IT des métiers et d'ouvrir enfin la voie vers une collaboration plus fluide en matière de gestion des traitements des données personnelles.
- **Opportunité de Transversalité :** indispensable pour tout projet transverse de transformation, le projet RGPD permet de mettre autour de la table de nombreuses parties prenantes : juristes, contrôleurs internes, managers, métiers, le support comme le marketing, l'IT, le RSSI, les achats, les sous-traitants, …
- **Opportunité de Transparence :** une vertu essentielle du dispositif est de mettre à disposition des personnes détenteurs de données personnelles un certain nombre d'informations les concernant et sur lesquelles ils ont désormais des droits : consentement, rectification, effacement, …
- **Opportunité de Confiance client :** les clients de l'entreprise conforme au règlement se sentent en confiance car ils auront la certitude que l'ensemble de leurs données seront préservées en termes de confidentialité, d'intégrité et de disponibilité. Cette confiance accordée est sans conteste un élément différenciant.
- **Opportunité de Partenariat :** la relation client-fournisseur est effacée pour laisser place à une vraie relation de confiance entre l'entreprise responsable des traitements et ses co-traitants.

Un nouvel enjeu : le Maintien en Condition de Conformité !

Il ne s'agit plus pour les organisations ayant fait le pari d'une première mise en conformité « a minima » pour mai 2018 d'en rester-là ; une feuille de route et un plan d'action continueront de générer des projets et à mobiliser des ressources dans l'entreprise afin de satisfaire l'ensemble des exigences requises. Le prochain challenge sera donc de maintenir le dispositif de conformité RGPD dans le temps et pour cela il sera nécessaire d'outiller et d'industrialiser notamment par la mise en place de nouveau processus.