IT-expert magazine

RGPD : quelles actions à J-100 jours ?

09 Feb 2018 - Alain Bensoussan, données, GDPR, protection, Règlement, RGPD, sécurité
by Aurelie Magniez

Les dispositions du Règlement européen sur la protection des données (RGPD) seront directement applicables dans les Etats membres de l'Union européenne le 25 mai 2018. Il reste moins de quatre mois aux entreprises pour se préparer à cette échéance que certains n'hésitent pas à comparer au Big bang de l'an 2000.

Avant l'été 2017, la moitié des entreprises déclarait ignorer les problématiques induites par la mise en conformité. Selon certaines études, deux tiers n'avaient pas nommé de DPO et près de la moitié ne savaient pas du tout si elles seraient conformes à temps. Depuis l'automne, la prise de conscience est réelle, qui s'est encore accrue au le 1er janvier 2018. Mais une chose est sûre : il est plus que jamais urgent pour les entreprises d'anticiper ce texte qui va modifier en profondeur les règles applicables à l'environnement digital des entreprises. Décryptage.

Le RGPD : un champ d'application

Le RGPD s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens.

Le périmètre du RGPD est donc particulièrement large puisqu'il couvre les entreprises et organisations qui utilisent ou stockent des informations personnelles des citoyens européens et de personnes physiques dans l'Union européenne ou de sociétés opérant au sein de celle-ci.

C'est donc la quasi-totalité des entités (entreprises privées, organismes publics et associations) traitant des données personnelles de citoyens européens qui sont concernées par le Règlement, soit la plupart des organisations partout dans le monde.

Ce que prévoit le Règlement

Ce texte impose aux entreprises de se plier à de nouvelles obligations. Celles-ci devront principalement :

- réaliser des analyses d'impact avant la mise en œuvre d'un traitement de données pouvant présenter des risques pour les droits et libertés des personnes ;
- prendre en compte la protection de la sécurité des données dès la conception du traitement de données concerné ;
- être en mesure, à tout moment, de démontrer la conformité du traitement avec le RGPD.

Les sanctions encourues

Il s'agit évidemment de l'enjeu majeur de la réforme : la Cnil, autorité de tutelle, pourrait être amenée à infliger des amendes pouvant atteindre 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires mondial annuel d'une entreprise.

Un effet positif en termes d'image

Mais la mise en application du RGPD devrait aussi et surtout avoir un effet positif : en ce qu'il renforce les obligations de sécurité des entreprises, le nouveau texte donne ainsi à leurs clients l'assurance d'un niveau de protection accru pour le traitement de leurs données personnelles. Au plan de la communication, le RGPD, qui exige le niveau de protection des données personnelles le plus élevé au monde, permet ce faisant d'accroître également la confiance de ses partenaires et collaborateurs, et de renforcer sa position concurrentielle.

Quelles actions à J-100 jours ?

Afin de mettre à profit les 100 jours qui restent jusqu'au 25 mai 2018, les organisations seront inspirées de respecter cinq priorités :

1. Adopter une **"posture" Informatique et libertés volontaire**, visible et insistante, tendant à se conformer aux obligations découlant à la fois de la loi informatique et libertés et du RGPD. Ceci par le biais d'une décision hiérarchique forte de mise en conformité, dont la démarche doit être initiée par la direction générale et entraîner l'ensemble des services pour devenir une nouvelle culture d'entreprise.
2. Mettre en place une organisation pour assurer la compliance RGPD au sein de l'entreprise. Il faut pour cela désigner un « chef d'orchestre » : ce sera, dans certaines situations, le Data protection officer (DPO) ou délégué à la protection des données, nouveau "pilote" de la conformité et personnage clé de l'environnement digital des entreprises.
3. Une fois l'organisation définie, il convient de réaliser un "diagnostic", véritable état des lieux destiné à établir une analyse des éventuels d'écarts de conformité. A la suite de celle-ci, les zones de risque seront identifiées, ce qui est une étape indispensable.
4. Se doter des outils permettant de "documenter" et de démontrer la politique Informatique et libertés : cela devient une nécessité en raison du principe de responsabilité ou d'*accountability* instauré par le RGPD. L'entreprise traitant de données à caractère personnel devra dorénavant, en cas de contrôle, être à même de démontrer qu'elle a mis en œuvre les mesures organisationnelles pour respecter le RGPD.
5. Enfin, le RGPD consacre la nécessité d'adopter une démarche dite de *privacy by design* et de *security by default*, qui modifient le pilotage des projets au sein des organismes en plaçant ces principes en amont de ceux-ci.

Alain Bensoussan
Avocat à la Cour
Cabinet Lexing Alain Bensoussan Avocats

Lexing Alain Bensoussan Avocats est un cabinet d'avocat entièrement dédié au droit de l'informatique et des technologies avancées depuis 1978. Le cabinet est distingué « Law Firm of the Year » pour l'année 2017 par la revue américaine Best Lawyers. Cette distinction est décernée pour la France dans la catégorie « Technologies de l'Information ».
Site web : https://www.alain-bensoussan.com/