Le désastre du GDPR ?

Difficile d'échapper au tsunami médiatique du GDPR - le nouveau règlement européen en matière de protection des données personnelles ! En fait, il ne se passe pas une semaine sans qu'une nouvelle publication martèle les obligations que le texte impose de respecter sous peine de lourdes sanctions.

A juste titre, en réalité, pour quatre raisons :

1. Le règlement concerne toutes les organisations (entreprises, administrations, associations, syndicats, PME, TPE….)
2. Il est complexe et va être difficile à implémenter
3. Il prévoit des sanctions considérables en cas de non application (4% du CA global du groupe / 20 millions d'euros)
4. Beaucoup d'acteurs pourront utiliser le GDPR dans leurs contentieux (syndicats, partenaires sociaux, salariés licenciés, associations de consommateurs, associations protection de la vie privée, clients mécontents…)

Des sanctions potentielles ?

Si l'on excepte les entreprises qui se sont déjà faites épinglées par la CNIL (banques, gros acteurs de l'Internet…), et les organisations qui traitent des données personnelles de santé, à ce stade, pourtant, rares sont les entreprises qui ont vraiment mis en oeuvre un plan de conformité.

En fait, aujourd'hui, il est plus réaliste de dire que le sentiment commun qui plane est que l'on attend de voir si les sanctions prévues par le règlement seront appliquées. En effet, pourquoi faire des dépenses considérables alors que les sanctions réelles prononcées n'ont été jusqu'à présent que de quelques minutes de chiffre d'affaire (ex : 150.000€ pour Facebook). Il faut dire que le laxisme de la CNIL a été tel en ce domaine qu'on en finissait par se demander ouvertement et publiquement dans quelle mesure il faut vraiment respecter la loi informatique et libertés ?

Les amendes prononcées contre Google, et Facebook ont, à ce titre, été vécues comme de véritables incitations à ne pas respecter la loi par de nombreuses organisations. Mais en fait, comment pourrait-il en être autrement ? La CNIL inflige quelques minutes de chiffre d'affaire de sanctions dans des affaires ou elle avait des pouvoirs considérablement plus étendus (et aurait pu par exemple faire effacer toutes les données collectées - art. 45, III de la loi). A quoi bon donc faire des frais, les sanctions étant dans tous les cas moins coûteuses qu'une mise en conformité…

Il résulte de cette politique qu'aujourd'hui, de nombreuses organisations attendent de voir dans quelle mesure la CNIL sera sérieuse dans l'application de ces sanctions. Or cette attente est un très mauvais calcul.

Le risque de sanctions ne vient pas de la CNIL

Non pas qu'il ne faille pas faire entrer la politique de sanctions de la CNIL dans une logique de gestion de risques juridiques. Au contraire, si les autorités ne sont pas sérieuses quant à l'application d'une règlementation, on ne voit pas en quoi les organisations auraient plus

de raison d'être sérieuses quant à mise en oeuvre. De nombreuses lois sont édictées pour de mauvaises raisons politiques et ne sont jamais appliquées en pratique.

Mais le GDPR est différent en cela qu'il prévoit des montants *démesurés* de sanctions (ex : 2 milliards d'euros de sanctions potentiels pour des entreprises comme Google, ou des entreprises du CAC40 en cas de non conformité).

Or ces montants considérables vont inviter un nombre important d'acteurs (autre que la CNIL) à utiliser le GDPR dans leurs contentieux : partenaires sociaux, syndicats, salariés licenciés, consommateurs insatisfaits... En fait, de nombreux contentieux classiques vont utiliser les ressources du GDPR pour faire augmenter considérablement les montants de sanctions.

En cela, le risque de contentieux est donc tout à fait réel et le fait que de nombreuses organisations y soient insuffisamment préparées est alarmant.

Mettre en place des actions de conformité

La seule chose qui va vraiment avoir un effet et réduire le niveau de risques juridiques en ce domaine, est la mise en oeuvre d'actions de conformité au nouveau règlement. Et c'est ce sur quoi les organisations vont devoir s'atteler.

S'il est difficile de viser une conformité à 100%, on peut néanmoins réduire substantiellement les risques d'une organisation en mettant en place une série d'actions relativement simples l'on résumera ici :

- Minimiser les données personnelles collectées
- S'assurer de disposer d'un fondement juridique du traitement
- Eviter de traiter des données sensibles
- Afficher les mentions légales
- Respecter le droit à la portabilité des données
- Mettre en place un registre de conformité
- Assurer la sécurité des données personnelles
- Maintenez un registre de violations de données personnelles
- Nommer un DPO
- Mettre en place un PIA pour les traitements les plus sensibles
- Ne pas transférer des données personnelles hors UE

La mise en place de ces actions évitera déjà le potentiel de désastre du GDPR.