SIX MOIS AVANT LA MISE EN ŒUVRE DU NOUVEAU RÈGLEMENT EUROPÉEN DE PROTECTION DES DONNÉES (GDPR)

# Pourquoi le GDPR fait peur aux entreprises

*Le nouveau règlement européen serre la vis en matière de protection des données personnelles. Six mois avant son entrée en vigueur, les entreprises prennent conscience de l'ampleur du travail à accomplir pour s'y conformer. Le point en 10 facteurs de stress.* **GILLES QUOISTIAUX**

Le 25 mai 2018, le nouveau règlement européen protégeant les données personnelles (GDPR) entrera officiellement en vigueur. Autant dire que pour les entreprises – toutes concernées à des degrés divers –, c'est le sprint final pour s'adapter à la nouvelle réglementation.

L'objectif principal du GDPR est de protéger la vie privée des citoyens européens dont les données privées sont collectées, stockées et traitées par les entreprises. A l'heure du big data et du *cloud computing* (informatique décentralisée), les banques de données sont devenues gigantesques, interconnectables, mais aussi vulnérables. L'Europe a donc décidé de donner un tour de vis supplémentaire pour inciter les entreprises détentrices de ces précieuses données – véritable pétrole numérique – à les manipuler avec précaution.

Votre date de naissance, vos appels téléphoniques, votre historique d'achats, votre fiche de paye, votre dossier médical, vos recherches sur Internet, etc. sont stockés quelque part sur des serveurs. Le nouveau règlement a pour but d'encadrer la détention et l'utilisation de ces données et d'uniformiser les règles en la matière sur l'ensemble du territoire européen.

Monstre bureaucratique pour les uns, simple réécriture de règles existantes pour les autres, le GDPR (*General Data Protection Regulation*) force les sociétés à se poser des myriades de questions en amont pour qu'elles soient prêtes le jour J. Pour leur apporter des réponses, ce ne sont pas les conseillers qui manquent. Ces derniers mois, on ne compte plus les séminaires, colloques et autres tables rondes consacrées au GDPR. Les avocats et consultants se sont emparés du sujet et tentent de sensibiliser les entreprises. Au fur et à mesure que l'échéance approche, l'angoisse monte. Voici leurs 10 plus grandes craintes:

## 1. Des sanctions indigestes

C'est le véritable épouvantail du nouveau règlement européen. Les amendes en cas d'entorse au GDPR pourront, dans certains cas, grimper jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires. Le calcul des sanctions pécuniaires est calqué sur la détermination des amendes exigibles en droit de la concurrence. Le GDPR va même un cran plus loin, explique Tanguy Van Overstraeten, associé chez Linklaters, qui dirige notamment la pratique protection des données de la firme : « En matière de concurrence, les amendes sont imposées par rapport au chiffre d'affaires réalisé dans une division en particulier. Par contre, au niveau du GDPR, les amendes concernent un pourcentage du chiffre d'affaires total du groupe. Elles pourraient donc être encore plus importantes. Ces sanctions sont prises très au sérieux par nos clients. C'est un important incitant à se mettre en conformité ». D'autant qu'au-delà de ces amendes sonnantes et trébuchantes, l'arsenal de sanctions est assez large. Les autorités de contrôle pourront, par exemple, confisquer des équipements ou encore interdire temporairement ou définitivement le traitement de certaines données. Dernière sanction « indirecte » : l'atteinte à l'image de l'entreprise si celle-ci est prise en défaut de légèreté dans le traitement des données personnelles de ses employés ou de ses clients.

## 2. Des profils inédits à trouver dans l'urgence

Dans le sillage du GDPR, un nouvel acronyme vient d'apparaître : le DPO ou *Data Protection Officer*. Certaines entreprises (pas toutes) devront nommer d'ici mai prochain un responsable de la protection des données. Ce DPO est un spécialiste du cadre légal entourant la gestion des données personnelles. Mais c'est aussi un spécialiste de la sécurité informatique. Cerise sur le gâteau : vu la particularité de sa fonction, le DPO doit être « indépendant » et ne peut pas dépendre hiérarchiquement de certains départements comme le marketing, pour éviter toute forme d'influence sur ses décisions. « C'est un mouton à cinq pattes », ironise Jacques Folon, associé chez Edge Consulting, une société de conseil qui s'est spécialisée dans l'accompagnement des entreprises pour l'implémentation du GDPR. Les entreprises les plus prévoyantes se sont précipitées sur les profils correspondant à ce descriptif de fonction, provoquant une pénurie d'experts. Du coup, des formations certificatives ont été mises sur pied en urgence par différentes écoles, comme l'ICHEC, la VUB ou Solvay, afin de donner des clés aux apprentis DPO. Autre solution pour les entreprises qui n'ont pas besoin d'un expert à temps plein : solliciter des DPO externes, qui peuvent travailler pour plusieurs clients. C'est ce que proposent désormais des sociétés de conseil spécialisées comme Edge Consulting ou GDPR Agency.

## 3. Former rapidement le personnel

Les connaissances du DPO ne suffiront pas pour mettre en place les nouveaux dispositifs en matière de protection des données requis par le GDPR. Pour que cela percole, une partie du personnel devra être formée. L'application du nouveau règlement a des impacts qui vont bien au-delà de la « simple » adaptation juridique de certains documents internes. « Environ 20 % du travail est d'ordre juridique. Le reste, c'est du *change management* », pointe Jacques Folon (Edge Consulting). Le GDPR suppose de repenser les processus internes relatifs au traitement des données. Alors qu'auparavant les entreprises étaient censées notifier leurs politiques de gestion des données personnelles à la Commission de protection de la vie privée (ce qu'elles ne faisaient pas toujours...), elles devront à l'avenir démontrer, si on les sollicite, qu'elles ont pris les mesures adéquates pour protéger lesdites données. « La logique est inversée. Les entreprises auront la charge de la preuve », explique Emmanuel Plasschaert, avocat associé chez Crowell & Moring.

## 4. Des tonnes de données à analyser

Les avocats et consultants que nous avons contactés sont unanimes : la première mesure à mettre en place pour faire face au GDPR est un audit interne de la société en matière de gestion des données. Toutes les données ne se valent pas et ne doivent pas être soumises aux mêmes mesures de protection. De même, toutes les entreprises n'ont pas la même utilisation des données qu'elles détiennent. « Je classe les entreprises en trois catégories, détaille l'avocat spécialisé Emmanuel Plasschaert (Crowell & Moring). Tout d'abord, celles ➤

dont le *business model* est axé sur les données comme Facebook ou Google. Ensuite, les entreprises qui traitent des données sensibles comme celles des hôpitaux ou des banques. Enfin, toutes les autres entreprises, qui manipulent des données moins sensibles. Tout le monde devra se mettre en ordre, mais les obligations les plus lourdes pèsent sur les deux premières catégories.»

## 5. Un monstre administratif

Le nouveau règlement européen est une nouvelle source d'activité juridique dans le domaine de la compliance (conformité). Pour éviter les problèmes en cas de contrôle, les entreprises doivent adapter leurs documents et leurs processus internes au nouveau cadre légal. «C'est hyper administratif», reconnaît Jacques Folon (Edge Consulting). D'après le consultant, tout est une question d'organisation et de documentation. Toute mesure prise concernant le stockage et la gestion des données personnelles doit, idéalement, faire l'objet d'une trace écrite. Exemple: «Si une entreprise active dans le commerce électronique décide de conserver les données de ses clients pendant cinq ans après leur dernier achat, cette décision doit être motivée et archivée», note le consultant.

## 6. Alerte aux fuites de données

L'entreprise ne doit pas seulement démontrer qu'elle a pris les mesures nécessaires pour collecter et traiter correctement les données. Elle doit aussi se prémunir contre les fuites, en investissant dans la cybersécurité. En cas d'attaque criminelle ou de perte de données personnelles, l'entreprise devra en avertir l'autorité de la vie privée dans les 72 heures. Ensuite, ce sera au tour des victimes d'être prévenues. Autant dire que les entreprises ont intérêt à mettre en place au préalable un système efficace de notification, pour ne pas être prises au dépourvu en cas d'évaporation de données.

## 7. Une autorité de contrôle plus féroce

L'arrivée du GDPR s'accompagne d'une transformation de la Commission de protection de la vie privée. Cet organe est actuellement une commission d'avis et de recommandations. Elle est habilitée à saisir la justice si elle constate des manquements à la législation en vigueur, ce qu'elle n'a pas manqué de faire dans des affaires toujours en cours, concernant notamment certains agissements de Facebook. Ses pouvoirs seront prochainement renforcés afin de se conformer aux nouvelles dispositions prévues par le règlement européen. Un projet de loi vient d'être déposé en ce sens au Parlement fin octobre. La Commission deviendra une Autorité de la vie privée, qui pourra prononcer des sanctions et imposer des amendes. Elle disposera d'un service d'inspection et d'une chambre contentieuse pour traiter les litiges. «Il faut se rendre compte que la Commission va devenir une vraie police de la protection des données», commente Christian Derauw, gérant de la société de conseil spécialisée GDPR Agency.

> ***«Il faut se rendre compte que la Commission de protection de la vie privée va devenir une vraie police de la protection des données»***
> *Christian Derauw, gérant de GDPR Agency*

## 8. Le risque de la «class action»

La récente loi belge autorisant les actions collectives pourrait trouver un terrain d'application dans les matières liées à la protection des données. Une association comme Test-Achats pourrait fédérer des consommateurs dont les données ont été divulguées ou manipulées illégalement. Un risque judiciaire et de réputation supplémentaire pour les entreprises.

## 9. Un coût, mais aucun bénéfice

Le GDPR ne sera pas neutre financièrement pour les entreprises. Les nouveaux processus à mettre en œuvre, la formation du personnel, les frais de consultance, les éventuels engagements, etc., leur coûteront du temps et de l'argent. D'après une étude conduite en mai dernier par la société de conseil SIA Partners, cette mise en conformité coûtera en moyenne 30 millions d'euros aux entreprises françaises du CAC 40. «Le retour sur investissement du GDPR? C'est zéro, indique Jacques Folon (Edge Consulting). L'objectif de la mise en conformité est de réduire le facteur de risque. La seule chose que l'on peut éventuellement en retirer est de faire une campagne marketing autour du fait que l'entreprise s'engage dans une démarche responsable de protection des données, ce qui démontre son engagement en termes de responsabilité sociétale.»

## 10. Les nombreuses incertitudes

Le règlement européen reste entouré de zones d'ombre. Ce n'est pas un hasard si les séminaires et conférences se multiplient sur le sujet, afin de tenter de décoder les passages les plus flous. Il n'est par exemple pas du tout évident de déterminer avec certitude quelles entreprises devront à l'avenir disposer d'une personne dédiée à la protection des données (DPO). C'est la raison pour laquelle un groupe de travail (baptisé G29), composé notamment de représentants des différentes autorités européennes de la vie privée, édite régulièrement des «lignes directrices», permettant de clarifier les dispositions sujettes à interprétation. Mais de nombreuses interrogations demeurent. Au grand bonheur des consultants et des avocats. ◉