NOUS & L'UMIH

N° 66 - Juin 2018

Protection des données : RGPD, une nouvelle façon de travailler

Le RGPD, Règlement général sur la protection des données personnelles, est applicable depuis le 25 mai. Application directe d'un règlement européen, il modifie en profondeur la façon dont les entreprises conservent et gèrent leurs données et celles de leurs clients. Bien au-delà du cadre qui existait jusqu'alors avec la loi Informatique et Libertés de 1978. Il introduit de nouveaux droits pour les personnes, qui ont pour corrolaire de nouvelles obligations pour toutes les organisations (entreprises, asociations collectivités,...) sous peine de lourdes sanctions financières. À l'heure où les Gafa (Google, Amazon, Facebook, Apple) s'approprient des masses de données personnelles et où explose la cyber-criminalité, ce surcroît de protection bénéficie à tout un chacun. Le récent scandale Cambridge Analytica/Facebook illustre le risque de détournement d'informations personnelles et la nécessité de transparence quant à l'utilisation des données. Et bien qu'il apparaisse contraignant pour les entreprises, le RGPD signifie avant tout pour elles l'adoption de nouvelles pratiques. Plus respectueuses des individus et de leur vie privée, elles doivent aussi les conduire à s'adresser à leurs clients, prospects, partenaires et sous-traitants avec plus d'efficience.

Le RGPD est un règlement européen qui vise à resserrer le contrôle quant à la protection et au respect des données personnelles et de la vie privée. Il est entré en vigueur le 25 mai dernier, et s'impose désormais aux entreprises, aux associations, aux collectivités, à l'administration, à toute entité traitant des données à caractère personnel. Celles-ci auraient tort de l'ignorer. L'objectif de cette réglementation, applicable à tous ceux ayant une activité économique dans l'espace européen, est de protéger les données personnelles des citoyens contre tout usage mercantile ou/et frauduleux.

Le souci de protéger les données s'explique au regard de la sauvegarde des libertés, mais aussi de l'explosion de la cyber-criminalité. Les entreprises qui détiennent des données sur les personnes s'exposent à les voir dérobées et utilisées à des fins illicites. Il est à noter que *« les hôtels sont une catégorie fortement ciblées par les cyberpirates, et comptent une part importante des 67 000 entreprises françaises qui ont porté plainte pour vol de données en 2017 »* explique Olivier Gourio, expert en cyber-sécurité des PME, fondateur d'Espar System qui nous a guidé sur ce dossier.

Depuis le 25 mai, ce qui change surtout pour les entreprises, c'est que, d'un point de vu juridique, elles se voient responsables de la protection des données personnelles qu'elles détiennent. Elles ont, à ce titre, une obligation de résultat. La grande question qui s'ouvre alors est de savoir de quels moyens elles disposent pour satisfaire ces obligations.

Données personnelles sensibles ou non

Par « données personnelles », on comprend toutes les informations qui se rapportent à une personne physique identifiée, directement ou indirectement : nom, numéro de téléphone, sexe, adresse courriel, adresse IP, numéro d'immatriculation, données de localisation, sans parler des données sensibles telles que des éléments physiques, médicaux, génétiques, économiques, etc. Rapporté aux CHRD, sont en particulier concernées, mais pas uniquement : les données clients des hôtels et restaurants. C'est ce que l'on appelle communément les **fichiers clients**.

De nouvelles obligations pour les entreprises à l'égard des individus

Les principales nouveautés introduites par le RGPD sont l'apparition de nouveaux droits pour les individus, qui sont autant d'obligations à respecter par les entreprises détentrices de données à caractère personnel. Notamment :

- Le droit à la **portabilité** : tout individu peut récupérer toutes les données le concernant auprès de n'importe quel organisme pour les réutiliser comme bon lui semble.
- le **droit à la limitation du traitement** : une personne physique peut exiger la limitation du traitement de ses données, contraignant l'entreprise à stocker ses données sans les utiliser. Ce droit ne peut se faire valoir que si le traitement est illicite et/ou si les informations récoltées sont inexactes.
- Le **droit à l'oubli** offre à toute personne physique la possibilité d'obtenir l'effacement de toutes les données le concernant auprès d'un organisme, par retrait du consentement, par injustification des données récoltées, opposition au traitement, etc.

Comme pour toute règle, quelques exceptions sont à connaître ainsi, le droit à l'oubli ne s'applique pas aux traitements répondant à des objectifs d'archivage scientifique, historique ou nécessaires à l'intérêt public.

- le **droit à l'information** permet à tout individu d'être tenu informé dès lors qu'il y a collecte de ses données même si celles-ci ont été obtenues auprès d'une tierce personne.
- le **droit d'accès** stipule qu'une personne a le droit d'obtenir une confirmation quant à l'état de ses données (sont-elles ou non traitées ?) et une copie de ses données.
- le **droit de rectification** permet de demander à compléter ou à rectifier ses données.
- le **droit d'opposition** consiste à pouvoir dire non à un traitement de données à caractère personnel, à tout moment ou à s'opposer à l'utilisation marketing de ses données.
- le **droit à la communication** d'une violation de données à caractère personnel oblige le responsable de traitement à prévenir toute personne dont les données auraient été violées. Le RGPD généralise l'obligation de notification des failles de sécurité à la CNIL et impose une obligation de communication aux personnes victimes de violation de leurs données personnelles.

© Nata-Lia - Shutterstock

Vous êtes garant de la protection des données collectées, celles-ci restent à disposition des personnes vous les ayant confiées.

© Monkey Business - Shutterstock

Concernant votre clientèle, il vous faudra recueillir son consentement explicite afin de conserver les données qu'elle vous a confiées afin d'être en conformité avec le RGPD.

Qu'est-ce que cela implique immédiatement pour vous ?

Tout d'abord depuis le 25 mai, vous devez mettre en avant les droits des individus sur votre site et la démarche pour les faire valoir. **Ensuite, il vous est défendu de conserver ou d'utiliser les données que vous possédez dans un but de démarchage.**

Des années de données collectées se trouvent ainsi interdites d'utilisation. C'est notamment le cas si vous vous adressez à vos clients par envoi de courriels, à moins que ceux-ci ne vous aient fourni un consentement explicite et justifiable.
Attention, si vous recevez une demande qui vise à faire valoir un de ces droits, vous devez y répondre au plus tard un mois après.

Aussi, vous devez avertir explicitement les visiteurs de votre site de la collecte de données, leur demander leur consentement et leur exposer leurs droits **(l'absence de réponse négative ne vaut pas consentement).**

Les CHR particulièrement exposés

Le risque est fort parce que les entreprises ne sont pas propriétaires de leurs outils de travail. C'est vrai en particulier des outils PMS sur lequel se trouve en général le fichier clients. En cas d'attaque informatique (cryptage, virus…), le risque est multiple. Outre la perte des données de réservation et du fichier clients, avec ses conséquences économiques, il existe un risque pénal et civil pour l'entreprise. En effet, **une personne, dont les données se trouveraient rendues publiques, serait fondée à poursuivre l'entreprise victime de la cyberattaque avec la possibilité pour les personnes lésées d'ouvrir une action collective.**
Un changement capital, car la responsabilité est partagée entre le fournisseur de PMS et son client avec l'obligation de chacunes des parties de s'assurer de la mise en conformité de l'autre.
Cette obligation de sécurisation est générale et s'applique jusqu'à des domaines auxquels on ne pense pas forcément. Olivier Gourio signale l'exemple-type du cabinet comptable auquel vous confiez la gestion de la paie de vos salariés. *« Imaginons que des pirates informatiques s'attaquent à ses ordinateurs et dérobent les données concernant vos salariés. Non seulement, vous devrez être en mesure de prouver que vous avez veillé à faire appel à un prestataire ayant mis des moyens de protéger les données, mais vos salariés dont les données ont été dérobées doivent être avertis par le cabinet victime du piratage. Sans compter la possibilité qu'ont les personnes lésées de se retourner contre le prestataire et contre vous ».*

Que faire tout de suite pour se mettre en conformité ?

La réponse se résume ainsi : établir la documentation prouvant votre conformité en gardant à l'esprit que **l'entreprise a une obligation de résultat en la matière.**

- Recenser vos bases données existantes : clients, salariés.
- Identifier leur origine, finalité, destination et durée de conservation.
- Vérifier que ces données ont été collectées légalement au regard du RGPD (et les détruire si ce n'est pas

5 actions suggérées par la CNIL

Nomination d'un délégué à la protection des données (DPO) interne ou externe
La CNIL le recommande mais il ne s'agit pas d'une obligation. Il s'assurera de la conformité et encadrera les traitements de données. Il sera l'interlocuteur privilégié de la CNIL en cas de contrôle.

Mise en place d'un registre de traitement des données
Les entreprises qui traitent des données devront dresser un registre des données recensant le type de traitement, les catégories de données traitées, l'objectif et la finalité des traitements, l'origine des données ainsi que leur destination en cas de transfert. Les sous-traitants sont soumis à la même obligation.

Analyse d'impact
Certaines entreprises doivent régulièrement évaluer les risques encourus par les droits et libertés des individus qui sont l'objet du traitement de données, ainsi que les actions mises en place pour éviter les risques. Cette analyse doit être effectuée régulièrement avec l'aide du responsable du traitement des données et du délégué à la protection des données.

Organisation d'un processus interne en faveur de la protection des données
Chaque entreprise doit garantir la mise en place de procédures de confidentialité et de sécurité de haut niveau. En cas de violation ou de fuite de données, vous avez 72 heures pour en informer la CNIL ainsi que les personnes concernées. *« Un simple anti-virus ne suffit pas »* alerte Olivier Gourio.

le cas, sachant que, outre l'utilisation, le stockage de données collectées en infraction au RGPD est illicite).
- Identifier les processus et dispositifs de collecte (formulaires, réseaux sociaux, ainsi que le type de données récupérées par tous ces dispositifs).
- Vérifier que vos sous-traitants sont en adéquation avec le RGPD.
- Nommer un responsable de la protection des données (v.infra).
- Mettre à jour les mentions légales de votre site.

En cas de **contrôle de la CNIL**, l'entreprise doit prouver sa conformité (via le responsable du traitement) en présentant les pièces suivantes :
- registre de traitement ;
- analyse d'impact ;
- présentation des mesures de protection des données exportées hors UE ;
- modèles de recueillement de consentement des individus ;
- procédures relatives à l'exercice des droits des individus quant à leurs données ;
- contrats entre différents acteurs pour définir la responsabilité de chacun ;
- procédures prévues en cas de violation ou de fuite de données.

Olivier Gourio, fondateur d'Espar System.

Se faire accompagner par des spécialistes

La mise en conformité au RGPD est pour le moins fastidieuse. C'est pourquoi les entreprises qui gèrent d'importantes bases de données ont intérêt à se faire accompagner par des spécialistes, tant sur le plan technique que juridique. C'est une prestation que proposent un certain nombre d'entreprises dont Espar System (société de services et de technologies dont la mission est d'assurer la cyber sécurité des PME européennes) pour les hôteliers, les restaurateurs et leurs fournisseurs, au moyen de plusieurs modules. L'un consiste en une évaluation de l'exposition de l'entreprise au RGPD et aux risques Cyber. Un autre est un service Sécurité Premium en partenariat pour l'ensemble du parc informatique des PME du CHR incluant l'anti-virus, l'anti-encryptions, l'anti-phishing des données (RGPD), l'anti-renommage et la mise à jour en temps réel de l'OS et des logiciels... Espar System améliore la protection des ordinateurs de ses clients et forme les salariés à devenir plus vigilants en matière de cyber risques. ■ **www.espar6.com**

Désigner un délégué à la protection des données (DPO)

La désignation d'un délégué à la protection des données n'est pas obligatoire pour des entreprises du secteur CHRD. La CNIL recommande toutefois de désigner une personne disposant de relais internes chargée de s'assurer de la mise en conformité du règlement européen.

De nouvelles mentions légales sur votre site

« L'objectif poursuivi par le RGPD est la transparence vis-à-vis de l'internaute qui visite votre site » rappelle

... un peu de légèreté

- RGPD : pas de collecte de données personnelles sans l'accord explicite des intéressés -

Olivier Gourio. Une page sur votre site doit être consacrée à informer sur le traitement des données, sa finalité, l'utilisation, le temps de conservation ainsi que les droits que possèdent les personnes sur leurs données et leur procédure d'application.

De lourdes sanctions en cas de non-conformité

Les infractions au RGPD sont lourdement sanctionnées au plan financier : jusqu'à 20 000 000 euros d'amende ou 4 % du chiffre d'affaires mondial. À cela s'ajoute un impact conséquent sur la réputation de l'établissement. Durant les premiers mois de la mise en application du RGPD, il importe surtout que les entreprises aient mis en route le processus qui les conduira à respecter leurs nouvelles obligations et qu'elles soient en mesure de le démontrer.

L'impératif d'adopter des réflexes de sécurité dans l'entreprise

Ce qui change, aussi, et surtout, avec le RGPD, c'est une autre approche de la notion juridique de responsabilité de l'entreprise par rapport aux données qu'elle détient. Sa responsabilité est en effet engagée dès lors que les données personnelles qu'elle détient sont dérobées et qu'elle ne peut prouver qu'elle avait consacré ses meilleurs efforts en vue d'assurer sa sécurité informatique.

« D'abord, penser sécurité à chaque instant » conseille Olivier Gourio. *« Les collaborateurs peuvent être le maillon faible ou au contraire la défense avancée de l'entreprise selon qu'ils sont formés aux bonnes procédures et qu'ils les respectent. Ce qui signifie par exemple s'empêcher de visiter des sites peu sécurisés en même temps que le logiciel PMS est ouvert (cas du veilleur de nuit). »*

Il s'agit aussi d'éviter systématiquement de se connecter au wi-fi public avec son téléphone ou un ordinateur.

Autre geste simple : éteindre son ordinateur en quittant son lieu de travail, tout comme les photocopieurs qui gardent en mémoire tous les documents qu'ils copient et scannent, sans oublier qu'ils sont équipés d'une boîte courriel.

Même si cette protection est loin d'être suffisante, il convient d'installer un antivirus (les versions gratuites ont des limites) et/ou le mettre à jour, tout comme les logiciels utilisés.

Les mots de passe doivent être changés régulièrement et il faut utiliser des complexes (de 6 à 8 caractères avec au moins une majuscule, un chiffre, un caractère spécial). Dans certain cas aussi, il faut chiffrer les données.

Enfin, face au risque de piratage, l'entreprise doit mettre en place une procédure de sauvegarde régulière et de récupération des données en cas d'incident technique.

Une nouvelle façon de travailler votre marketing direct

Avec le RGPD, le marketing quantitatif laisse la place à un marketing qualitatif. Il oblige les professionnels à repartir de zéro pour constituer une nouvelle base de données licite (explicitement consenties) et pertinente.

L'arrivée du RGPD n'a pas que des désavantages. Vous pouvez y voir une opportunité pour renforcer vos relations clients.

En effet, en adoptant la transparence exigée par le RGPD, vous verrez la confiance de vos clients renforcée considérablement.

Or, en marketing, posséder la confiance de ses clients vaut tout l'or du monde. Un client qui vous fait confiance est un client fidèle et un prescripteur hors pair.

Finalement, le RGPD est avant tout une nouvelle manière de travailler. Une nouvelle relation client commence ! ■ **Sébastien Hobbels**

À faire dès maintenant

1 - Recenser les fichiers dans un registre des fichiers

Pour chacun d'eux, préciser :
- la finalité du traitement (fidélisation client, gestion du personnel, etc.) ;
- les catégories de données utilisées (ex : nom, adresse, courriel...) ;
- le destinataire qui a accès aux fichiers (hébergeur du site internet, service informatique, etc.).

N.B. : N'ont pas à être mentionnées dans le registre les traitements de données seulement occasionnels.

2 - Faire le tri

Je trie mes données. Je prends chaque fiche et je vérifie que :
- les données traitées sont nécessaires à mes activités. Inutile de savoir si mes salariés ont des enfants si en avoir n'a aucun effet sur les rémunérations ;
- parmi les données traitées, il n'en est pas qui sont sensibles (opinions politiques, syndicales, orientation sexuelle, etc.) ;
- seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- mes délais de conservation ne vont pas au-delà de ce qui est nécessaire.

3 - J'informe les personnes concernées

Pour prouver le respect de l'obligation de transparence, doivent apparaître clairement :
- la finalité : pourquoi je collecte les données ;
- le fondement juridique pour traiter ces données ;
- les personnes ayant accès aux données ;
- le délai de conservation ;
- les modalités d'exercice des droits ;
- le transfert de données hors UE.

4 - Sécuriser les données

Quatre règles d'or :
- installer un antivirus (les versions gratuites ont des limites) et/ou le mettre à jour régulièrement, de même que les logiciels ;
- changer régulièrement les mots de passe et en utiliser des complexes (de 6 à 8 caractères avec au moins une majuscule, un chiffre, un caractère spécial) ; comme £ ou & ;
- dans certains cas, chiffrer les données ;
- mettre en place une procédure de sauvegarde régulière et de récupération des données en cas d'incident technique.