LE SECRET À L'HEURE DU RGPD

Alain BENSOUSSAN
Avocat au Barreau de Paris | Président d'Honneur

À quelques semaines de son entrée en vigueur, le Règlement général sur la protection des données (RGPD) peine encore à mobiliser les cabinets avocats, en dépit des actions de sensibilisation que mène le Conseil national des barreaux depuis quelques mois.
Principale raison : nos confrères considèrent dans leur grande majorité qu'en matière de protection des données personnelles, le secret professionnel suffit et les dispense de se conformer au nouveau Règlement européen. Or, c'est précisément pour cette raison qu'ils sont concernés et doivent redoubler de vigilance.

LE RGPD, C'EST MAINTENANT !

Le Règlement général sur la protection des données (« *RGPD* » ou « *GDPR* » en anglais), adopté le 27 avril 2016, sera directement applicable dans l'ensemble des États membres le 25 mai 2018.

Les cabinets d'avocats sont concernés par cette réforme qui impacte en profondeur l'environnement digital de l'ensemble des entreprises : ceux-ci sont évidemment amenés à mettre en œuvre un nombre important de traitements qui peuvent s'avérer d'une particulière sensibilité du point de vue du droit des données personnelles.

Ceci nécessite un encadrement particulier de ces traitements notamment en termes de sécurité, de confidentialité, de loyauté... Mais aussi et surtout de protection au regard du secret professionnel auquel nous sommes astreints.

Or, si certains sont déjà sensibilisés au sujet, la grande majorité de nos confrères estiment que le secret professionnel suffit et les dispense de se conformer au RGPD.

Pourtant, dès lors qu'ils traitent de la donnée client, les avocats sont concernés par le RGPD.

Ils le sont tout autant pour leur gestion RH, la surveillance de leurs locaux ou encore dans le cadre de leur politique de marketing & communication.

Ceci passe notamment par l'information des personnes concernées et la nécessité de mentions particulières notamment dans les conventions d'honoraires.

Il convient également d'insérer des clauses particulières dans les contrats de sous-traitance conclus avec les prestataires auxquels ils recourent.

Du point de vue de la sécurité, il leur est nécessaire d'assurer une bonne gestion de l'accès aux locaux et au système informatique, de procéder à l'archivage des dossiers de leurs clients.

Pour chacun des traitements mis en œuvre par un cabinet d'avocats, celui-ci doit déterminer une durée de conservation des données qui soit adaptée au regard de la finalité de chacun d'eux.

Autant d'enjeux qu'ont bien compris nos instances représentatives, comme le démontre la parution, au moment où nous bouclons ces lignes, du Guide pratique « *Les Avocats et le Règlement général sur la protection des données (RGPD)* » rédigé par le CNB, le Barreau de Paris et la Conférence des bâtonniers (1ère éd., mars 2018).

Depuis quelques semaines, les Ordres et les écoles d'avocats se saisissent de cette question notamment en organisant des formations dédiées à l'accompagnement des avocats dans la mise en conformité de leur cabinet avec les exigences du RGPD.

DE NOUVELLES OBLIGATIONS POUR LES AVOCATS

De façon générale, le RGPD va imposer aux cabinets de se plier à de nouvelles obligations, parmi lesquelles :

- l'obligation, à tout moment, d'être en mesure de démontrer la conformité de leurs traitements (principe de responsabilité ou d'*accountability*) ;
- la prise en compte de la protection de la sécurité des données, tant logique que physique, du traitement de données concerné ;
- l'obligation de notifier à la CNIL toute violation de données à caractère personnel.

SE POSER LES BONNES QUESTIONS

Avec le RGPD, les avocats doivent intégrer les bons réflexes d'une véritable posture Informatique et Libertés.

En premier lieu, il convient de s'interroger : le cabinet réalise-t-il des traitements de données personnelles qui l'assujettit à la réglementation Informatique et Libertés du fait de leur nature, de leur portée et/ou de leur finalité ?

La réponse est évidemment positive comme au sein de n'importe quel organisme ou entreprise.

Rappelons qu'une donnée à caractère personnel est définie comme *« toute information permettant d'identifier une personne physique »*, soit directement (tel que le nom et le prénom, le numéro de sécurité sociale, son numéro de matricule...) soit indirectement (notamment par référence à des éléments qui lui sont propres : un identifiant en ligne, ou un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, économique, culturelle ou sociale, la fonction d'une personne, des données de localisation géographique...).

Dès lors que les données permettent de remonter à une personne physique et qu'il reste une possibilité d'identifier à qui ces données sont rattachées, celles-ci sont considérées comme ayant un caractère personnel.

La nouvelle réglementation s'applique à la mise en œuvre des traitements de données à caractère personnel, qu'il s'agisse :

- de fichiers ou bases informatiques (fichiers du personnel ou fichiers de clients) ;
- de systèmes faisant appel à d'autres technologies (téléphone, accès par badge, vidéosurveillance, etc.).

RECENSER LES TRAITEMENTS DE DONNÉES DU CABINET

Pour mesurer concrètement l'impact de la réglementation Informatique et Libertés et du RGPD sur son activité, l'avocat devra recenser de façon précise les traitements de données personnelles mis en œuvre au sein de son cabinet.

C'est l'étape préalable, nécessaire et primordiale dans le cadre de la mise en conformité au RGPD.

Elle permet de disposer d'une vue d'ensemble des traitements de nature à impacter les droits et libertés fondamentaux de clients, collaborateurs et partenaires du cabinet et permet de s'assurer que les traitements respectent l'ensemble des nouvelles obligations légales issues du RGPD.

La tenue d'un registre des traitements[1] pourra lui permettre de faire le point : dans le cadre du RGPD, les organismes doivent tenir une documentation interne complète sur leurs traitements de données personnelles et s'assurer que ces traitements respectent bien les nouvelles obligations légales.

Pour être en capacité de mesurer l'impact du RGPD sur son activité, il est nécessaire de recenser plus précisément :

- les différents traitements de données personnelles ;
- les catégories de données personnelles traitées ;
- les objectifs poursuivis par les opérations de traitements de données ;
- les acteurs (internes ou externes) qui traitent ces données : nécessité de clairement identifier les prestataires sous-traitants afin d'actualiser les clauses de confidentialité ;
- les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne.

Dès 2011, dans son Guide *« Les Avocats et la loi Informatique et Libertés »* rédigé en partenariat avec le CNB, la CNIL recensait les données dont dispose le cabinet qui pourraient être concernées :

- les traitements informatisés concernant les clients du cabinet ;
- les traitements informatisés concernant des clients potentiels ;
- les traitements constitués à des fins d'information de la clientèle ;
- les dossiers professionnels des salariés, anciens salariés ou collaborateurs ;
- les traitements relatifs au contrôle de l'accès aux locaux (badges électroniques, dispositifs biométriques ou encore vidéoprotection) ;
- le contrôle de l'utilisation d'internet et des messageries électroniques (communication électronique de pièces, anonymisation des décisions de justice).

En pratique, il est vivement conseillé de recenser vos différents traitements de données à caractère personnel via chaque support :

- les logiciels, les progiciels, les fichiers (au format Word, PDF, Excel) ;
- les matériels (serveurs, NAS, ordinateurs de bureau, ordinateurs portables, tablettes, disques durs, clés USB, etc.) sans oublier les données qui figurent chez des sous-traitants (les données à caractère personnel figurant dans vos emails, les fichiers figurant dans les dossiers partagés, Google Drive...), les données confiées à vos comptables... ;
- les supports et fichiers papiers (fiches papiers de liste clients, fiches papiers de listes de contact, bon de commande...).

DÉFINIR LA FINALITÉ DES DONNÉES PERSONNELLES COLLECTÉES

L'utilisation et le traitement de données personnelles doivent s'inscrire dans un but précis.

Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :

- collecte et traitement des données personnelles de manière loyale et licite ;

1. Les entreprises ou organisations de moins de 250 employés bénéficient d'une dispense de registre de traitements sauf lorsqu'elles tombent dans l'une des quatre hypothèses suivantes : le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées ; le traitement n'est pas occasionnel ; le traitement effectué porte sur des « données sensibles » ; le traitement effectué porte sur des données judiciaires (RGPD, art. 30).

- collecte uniquement pour des finalités déterminées, explicites et légitimes ; les données ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités ;
- données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs : seules les données adéquates et strictement nécessaires pour atteindre la finalité du fichier sont autorisées à y figurer ;
- conservation des données sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

On le voit, la mise en conformité avec le RGPD est un enjeu majeur, la CNIL pouvant être amenée à infliger des amendes particulièrement dissuasives (10 à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires mondial).

Mais sa mise en application devrait aussi et surtout avoir un effet positif puisqu'il renforce les obligations de sécurité, donnant aux clients, collaborateurs et partenaires l'assurance d'un niveau de protection accru pour le traitement de leurs données personnelles.

CONSEILS PRATIQUES
LES PRINCIPALES ACTIONS À METTRE EN PLACE AU SEIN DU CABINET

- **Assurer la sécurité de ses traitements de données personnelles**. Pour cela :
  - gérer les habilitations et sensibiliser les utilisateurs (définir des profils d'habilitation, supprimer les permissions d'accès obsolètes, rédiger une charte informatique à annexer au règlement intérieur...) ;
  - sécuriser les postes de travail (limiter le nombre de tentatives d'accès à un compte, installer un firewall, mettre à jour les antivirus...) ;
  - mettre en place une politique d'authentification des utilisateurs (identifiant unique à chaque utilisateur, politique de mot de passe utilisateur rigoureuse, etc.) ;
  - sauvegarder et prévoir la continuité d'activité ;
  - encadrer la maintenance ;
  - protéger le réseau informatique interne ;
  - tracer les accès et gérer les incidents ;
  - sécuriser les serveurs et les applications.
- **Informer ses clients et son personnel** (affichages de notes d'information : formulaire de collecte de données à caractère personnel ; clause ou notice d'information en matière de recrutement ; mention dans la convention d'honoraires, panneau d'information concernant la vidéo-protection, l'enregistrement de conversations téléphoniques et le contrôle d'accès biométrique...).
- **Gérer le site internet du cabinet** (contrôle des mentions obligatoires, notamment relatives aux droits des personnes ; consentement préalable de la personne concernée en matière de cookies...).
- **Bien choisir ses prestataires** (cf. le « *Guide sous-traitant* » disponible sur le site de la CNIL ; se renseigner sur le prestataire du *cloud* et les mesures de sécurité mis en place).
- **Être vigilant en matière de sollicitation personnalisée** : en matière de prospection par voie électronique, recueillir le consentement préalable à la collecte, sauf exception (personne déjà cliente et/ou prospection concernant des services analogues...).
- **Gérer les violations de données** : prévoir en interne un processus propre de gestion des incidents (cf. sur ce point le guide CNIL : « *Notifications d'incidents de sécurité aux autorités de régulation : comment s'organiser et à qui s'adresser ?* », 26 juillet 2017).