L’avocat et le RGPD

SECTION 1 - INTRODUCTION

La protection des données à caractère personnel présente un enjeu particulièrement sensible pour l’avocat. Les données auxquelles il a accès dans l’exercice de ses missions relèvent très souvent de la vie privée de ses clients ou de leurs proches ainsi que des parties adverses.

En outre, ces données sont souvent de nature sensible de sorte que la protection des données traitées par l’avocat est inhérente au lien de confiance l’unissant à son client et au respect de ses obligations déontologiques.

Le respect du secret professionnel, tel que défini par l’article 458 du Code pénal et des règles de confidentialité énoncées par le Code de déontologie, le conduit à une prudence particulière, mais ne peuvent suffire à garantir sa conformité aux dispositions relatives à la protection des données à caractère personnel et notamment le RGPD[1]. Ces règles impératives concernent aussi bien le traitement des dossiers papiers que digitalisés de l’avocat (Cloud, secrétariat, traducteur, etc.), que sa communication (site Internet, blog, consultation en ligne, etc.) ou encore son rapport à ses confrères, collaborateurs, stagiaires et son ordre.

Ce nouveau régime impose à l’avocat non seulement de respecter les principes généraux et les obligations énoncés dans le Règlement (Section 2), mais également d’être capable, à tout moment de prouver, autrement dit documenter, sa conformité (Section 3).

[1] Règlement (UE) no 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci -après Règlement général sur la protection des données ou RGPD).

L'avocat, auxiliaire de justice et garant du secret professionnel, doit se montrer particulièrement exemplaire en la matière.

SECTION 2. LES PRINCIPES GÉNÉRAUX ET OBLIGATIONS DU RGPD

En ses articles 5[2] à 11 le RGPD énonce les principes généraux qui doivent guider chaque traitement de données à caractère personnel de l'avocat. Ils se traduisent par des obligations concrètes visant à assurer la conformité au Règlement.

§1er. Principes de licéité et de finalité

Les literas a) et b) de l'article 5 du Règlement, fixent les principes de transparence, de loyauté, de finalité et de licéité du traitement. Il s'ensuit que chaque traitement doit impérativement avoir une finalité, déterminée, explicite et légitime, et être licite[3] pour ne pas entraîner une violation du Règlement.

Les bases de licéité sont limitativement énoncées à l'article 6 §1 du RGPD[4].

Parmi ces bases l'avocat doit déterminer celles appropriées aux traitements qu'il désire effectuer. Ce choix n'est pas anodin, notamment dans l'application des droits des personnes concernées qui en découle. D'autant qu'une base de licéité incorrecte est assimilée à une absence de base de licéité et est soumise à sanction.

---

[2] RGPD art.5

[3] Le principe de licéité du traitement n'est pas neuf, le Règlement reprend en son article 6, quasiment à l'identique les bases de licéité des traitements déjà listées au sein de la directive 95/46/CE, consolidant ainsi les avis du Groupe travail de l'article 29.

[4] RGPD art. 6 §1 *« Le traitement n'est licite **que si, et dans la mesure où**, au moins une des conditions suivantes est remplie :*

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

b) le traitement est **nécessaire à l'exécution d'un contrat** auquel la personne concernée est partie ou à **l'exécution de mesures précontractuelles** prises à la demande de celle-ci;

c) le traitement est nécessaire au respect d'une **obligation légale** à laquelle le responsable du traitement est soumis;

d) le traitement est **nécessaire à la sauvegarde des intérêts vitaux *(…)***

e) le traitement est nécessaire à **l'exécution d'une mission d'intérêt public ou** relevant **de l'exercice de l'autorité publique** dont est investi le responsable du traitement;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, *(…) »*

A titre d'exemple, si l'avocat décide de fonder la gestion de ses dossiers sur le consentement, il doit être capable de cesser ce même traitement si le consentement vient à être retiré[5], ce qui est rendu impossible dans le cadre de la défense en justice de ses clients. De manière générale, l'avocat bénéficie dans l'exercice de sa profession d'obligations légales. Elles sont par exemple énoncées dans le Code judiciaire, en sa qualité d'auxiliaire de justice lorsqu'il conclut ou réalise des actes de procédure[6].

Par ailleurs, lorsqu'il fait usage de données de catégories particulières[7] telles que les données relatives aux origines raciales ou ethniques, les opinions politiques, religieuses ou philosophiques, ou à l'appartenance à un syndicat, au casier judiciaire, à l'état de santé, l'avocat doit vérifier que l'une des conditions de l'article 9§2 est bien remplie.

A ce titre, le litera f) de cet article permet le traitement de ces données s'il est rendu « nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice (…) ».
En conclusion, il revient à l'avocat de procéder à un jeu de piste qui consiste à articuler les dispositions des articles 5, 6 et, s'il échet, 9 et 10 du RGPD.

Par ailleurs, la base de licéité ainsi que la finalité doivent faire l'objet d'une communication transparente vers les personnes concernées.

§2. Principe de transparence et de loyauté

Charte vie privée, formulaires de demandes des personnes concernées, politique des cookies pour son site internet, afin d'assurer l'obligation de transparence et de loyauté, l'avocat doit communiquer sur ses traitements vers les personnes concernées, notamment ses clients, ses employés, la partie adverse ou les personnes qui visitent son site internet, et ce, dès la collecte des données.

L'article 13 et 14 du Règlement énonce les mentions minimales que doivent comporter ces communications, telles que l'identité et les coordonnées de l'avocat ou de son cabinet, les finalités du traitement, la base juridique du traitement, les destinataires des données, la durée de conservation. AVOCATS.BE a mis à disposition un modèle de charte à adapter par l'avocat au regard de sa pratique. Il est conseiller de partager ce document à l'ouverture du dossier au même moment que les conditions générales

[5] Groupe de travail « Article 29 » sur la protection des données (ci-après, « G 29 »), « Avis no 15/2011 sur la définition du consentement », 25 novembre 2011, W.P. 187, p. 14 ; RGPD art. 7 ; en sus, le consentement doit répondre aux conditions énoncées par le Règlement, en ses articles 7 et 8 et être libre spécifique et informé.
[6] Elles se trouvent également dans les dispositions du livre III du Code de droit économique quand il gère sa comptabilité ou encore dans la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme quand il ouvre un dossier et prend l'identité de ses clients.
[7] RGPD art. 9 et 10.

de l'avocat ou du cabinet.

On y retrouve également les droits des personnes concernées. Ces droits sont les suivants, le droit d'accès en ce compris le droit de savoir si l'avocat traite ses données ; le droit d'avoir une copie des données traitées; le droit de rectification des données traitées; le droit d'opposition des données traitées ; le droit de limiter le traitement des données traitées; le droit à l'effacement des données traitées; le droit à la portabilité des données traitées; le droit de déposer une plainte auprès de l'Autorité de contrôle.

L'avocat doit donner suite à toutes les demandes dans les meilleurs délais et au plus tard dans le mois qui suit leur réception. Selon la difficulté de la demande ou le nombre de requêtes qu'il reçoit, ce délai pourra être prolongé de deux mois. Dans ce cas, il doit en avertir le demandeur dans le mois suivant la réception de la demande.

Enfin il existe une exception à l'obligation d'information « lorsque, et dans la mesure où, la personne concernée dispose déjà de ces informations »[8], ce qui est notamment le cas des données des avocats traitées par les avocats.

§3. Principe de minimalisation et de limitation de la durée

Le principe de minimisation ou limitation, des données et des traitements, énoncé à l'article 5 §1 c), est un principe[9] qui consiste, d'une part, à s'interroger sur la nécessité de traiter des données à caractère personnel pour atteindre les finalités recherchées par le traitement, et, d'autre part, à limiter le traitement des données au minimum, en ce qui concerne[10] les catégories de données traitées, les données traitées et la quantité de données traitées.

Il s'ensuit assez logiquement le principe de la limitation de la conservation énoncé à l'article 5 §1, e), selon lequel l'avocat n'est pas autorisé à conserver ou traiter les données à vie ou au-delà de la durée nécessaire pour réaliser les finalités du traitement.

Cette durée doit pouvoir être justifiée, de sorte qu'il est conseillé, mais pas obligatoire, de se fonder sur les délais légaux, tels que les délais de prescription de la responsabilité professionnelle, ou les délais de conservation comptable et fiscale.

[8] RGPD art. 13, § 4.

[9] Y. Poullet, « Chapitre 1 – Analyse critique du RGPD », in La vie privée à l'heure de la société du numérique, Bruxelles, Larcier, 2019, pp. 97 à 168.

[10] RGPD art. 25 et cons. 39 et 78.

Pour tout délai de conservation plus important que les délais légaux, il y aura lieu de documenter, les motifs justifiant la durée du délai.

Enfin, il est opportun de mettre en place et de documenter les mesures permettant de mettre fin aux traitements de manière effective et sécurisée dès la fin du délai de conservation.

§4. Principe de sécurité adéquate

L'avocat devra apporter une véritable attention à cette obligation, dans la mesure où il est amené à traiter des données de catégorie particulière. Il doit mettre en œuvre toutes les mesures utiles et nécessaires afin d'assurer un niveau de sécurité technique et organisationnelle adéquat, à savoir conforme à « l'état de l'art ».

À titre d'exemple, il doit limiter l'accès à ses locaux aux tiers en son absence ou en l'absence d'un membre de son équipe (ex : équipe de nettoyage, co-working,…), ne pas stocker ou archiver des dossiers ou documents contenant des données à caractère personnel dans des espaces accessibles à tous, installer des alarmes dans ses locaux, authentifier les utilisateurs par la mise en place d'un mot de passe assurant un niveau de sécurité suffisant, gérer les habilitations, supprimer les permissions d'accès obsolètes, le cas échéant rédiger une charte informatique, sécuriser l'informatique mobile : prévoir des moyens de protection pour les ordinateurs portables et les unités de stockage amovibles (clés USB, CD, DVD…), éviter d'y stocker des données à caractère personnel sensibles des clients, mettre en place des sauvegardes régulières, stocker les supports de sauvegarde dans un endroit sûr, etc.

Il devra aussi apporter une attention particulière à la formation donnée à son équipe, ses stagiaires, ses collaborateurs et employés.

Ces mesures doivent être documentées afin de prouver sa conformité.

Par ailleurs, il doit intégrer les concepts de protection des données dès la conception de nouveaux produits ou services et par défaut. Lorsque l'avocat fait évoluer ses pratiques, il doit s'interroger ab initio sur l'impact de l'évolution sur les données qu'il traite. Cela implique notamment l'intégration de dispositifs techniques de protection des données à caractère personnel et de mesures organisationnelles permettant de limiter les risques d'atteinte aux droits et libertés des individus.

SECTION 3. « ACCOUNTABILITY » OU « LA RESPONSABILISATION »

Comme son nom l'indique, le RGPD a pour objectif de moderniser le cadre européen de la protection des données à caractère personnel, notamment en renforçant les droits des personnes physiques à l'égard du traitement de leurs données à caractère personnel tout en assurant la libre circulation de ces mêmes données sur le territoire européen. L'interconnexion de ces objectifs se traduit notamment par l'introduction de la notion de « responsabilité comptable », plus connue sous le vocable anglais « *accountability* »[11] exprimée aux dispositions de l'article 5, § 2, du RGPD.

Il s'ensuit une inversion de la charge de la preuve et l'obligation pour l'avocat d'être capable à tout moment de prouver sa conformité. Pour ce faire, il doit documenter ses démarches et notamment : tenir des registres (§1er), réaliser des conventions avec les personnes ayant accès aux données (§2).

§1er. Les registres

Le registre est l'instrument que le règlement préconise en vue de se mettre en conformité et d'être capable à tout moment de prouver ses démarches.

Ainsi, il est recommandé de tenir divers registres : registre des traitements, registre des notifications de fuites, registre des demandes des personnes concernées, registre des sous-traitants, tous ces outils permettent de prouver sa mise en conformité au Règlement.

Le registre des traitements en qualité de sous-traitant ou de responsable des traitements et le registre des notifications des fuites de données à caractère personnel sont rendus obligatoire[12] par le règlement.

A. LES REGISTRES DES TRAITEMENTS

La réalisation des registres des traitements est une étape indispensable pour la mise en conformité au RGPD[13]. Ces registres sont les livres

[11] K. Rosier et A. Delforge, « Titre 15 – Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD », *in Le Règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018, p. 698.

[12] RGPD art. 30, § 1er, art. 30, § 2, art. 33 et 34.

[13] Cette obligation souffre tout de même d'exceptions pour les seules entreprises ou organisations qui

comptables de la gestion des données. Ils doivent être mis à jour régulièrement.

Le registre du responsable du traitement comporte à minima les informations suivantes[14] :

- Le nom et les coordonnées du responsable du traitement, le cas échéant le nom et les coordonnées du responsable conjoint, le cas échéant le nom et les coordonnées du D.P.D. ;
- Les finalités du traitement ;
- Les catégories de personnes concernées et le type de données ;
- Les destinataires ;
- Le cas échéant, les transferts de données hors de l'U.E. ;
- Les délais prévus pour l'effacement des données ;
- Une description des mesures de sécurité techniques et organisationnelles.

Le registre du sous-traitant doit contenir toutes les informations suivantes :

- Le nom et les coordonnées de chaque responsable du traitement pour lequel il agit, et le cas échéant, le nom et les coordonnées du ou des sous-traitant(s) pour le(s)quel(s) il agit, le cas échéant, le nom et les coordonnées du D.P.D. ;
- Les catégories de traitements effectués ;
- Le cas échéant, les transferts de données hors de l'U.E. ;
- Une description des mesures de sécurité techniques et organisationnelles.
- Les autorités de protection des données mettent à disposition des acteurs des modèles de registre en format XLS[15] ou World, qui sont assez classiques et faciles d'utilisation[16].

comptent moins de 250 employés et qui ne réalisent pas de traitements qui sont susceptibles de comporter un risque pour les droits et des libertés des personnes concernées ; ou ne réalisent des traitements qui sont purement occasionnels ; ou ne réalisent pas de traitements qui portent notamment sur les catégories particulières de données visées à l'article 9.1 du RGPD; ou ne réalisent pas de traitements qui portent sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 du RGPD.

[14] Commission vie privée, Recommandation no 06/2017 « relative au Registre des activités de traitements » (CO-AR-2017-011), 14 juillet 2017, pp. 11 et s.

[15] CNIL : exemple de registres : www.cnil.fr/fr/RGDP-le- registre-des-activites-de-traitement#1_le_ registre_du_responsable_de_traitement.

[16] AVOCATS.BE propose un modèle de registre à destination des avocats à télécharger sur son site mais **qui doit être adapté et complété** pour rendre compte avec exactitude de l'activité traitement propre à chaque avocat. (mesure de sécurité, …).

Le Règlement porte une attention soutenue aux failles de sécurité et aux violations des données à caractère personnel qui peuvent survenir. Une violation de données à caractère personnel est susceptible de causer aux personnes physiques concernées des dommages économiques ou sociaux importants, ou même un préjudice moral.

En cas de faille l'avocat notifie à l'Autorité de contrôle les violations constatées (fuites de données, accès non autorisé, pertes de données, etc.) sauf si la violation ne présente aucun risque. Cette notification doit se faire dans les septante-deux heures116 de la prise de connaissance de la faille.

Dans cette même période, il faudra aussi juger de la pertinence de notifier la faille aux personnes concernées. Le délai de réaction est court, très court.

À ce titre, il est suggéré de mettre en œuvre les mesures suivantes :

- Déterminer une personne/cellule de crise ;
- Formaliser une procédure de gestion des violations de sécurité.

Enfin et certainement, il y a lieu d'élaborer un registre documenté des failles dans la gestion des données à caractère personnel et de l'assortir de fiches de retours d'expériences. Ce registre permet d'une part en cas de contrôle de l'Autorité, de lui rendre compte et d'autre part d'optimaliser la gestion des données en réduisant les risques pour l'avenir.

§2. Les contrats

L'avocat doit aussi garantir que l'ensemble des personnes ayant accès aux données à caractère personnel qu'il traite, tant en qualité de responsable du traitement que de de sous-traitant, agissent conformément à ses instructions. Pour ce faire, il doit prévoir les accords nécessaires avec ces personnes.

S'agissant des personnes travaillant sous son autorité, comme ses employés, ou stagiaires-collaborateurs, une clause de confidentialité renforcée et assurant la conformité au RGPD suffit.

S'agissant de ses sous-traitants et responsable conjoint, de réaliser les conventions ad hoc telles conformément par le Règlement en ses articles 26 et 28.

A titre exemplatif, un cabinet exploitant sous licence un programme informatique avec un accès à distance pour son fournisseur, devra prévoir avec ce dernier une convention de protection des données. Il en va ainsi à l'égard de son secrétariat social, de la DP-A, ou encore son service postal. Dans la grande majorité des cas, ces sous-traitants ont déjà adapté leurs conditions générales en y intégrant les mentions requises à l'article 28 du RGPD.

SECTION 4. CONCLUSION

La mise en conformité n'est pas un processus simple et nécessite de la part de l'avocat, une prise de conscience des modalités de traitements qu'il met en œuvre ainsi qu'un changement d'habitude et la mise en œuvre d'une documentation à vocation probatoire.