RGPD : réflexions pour s'organiser et se mettre en conformité

Les informations que les cabinets sont amenées à connaitre, enregistrer et utiliser sont des informations par nature privées et sensibles (santé, vie professionnelle, casier judiciaire, opinions politique et religieuses…).

Notre profession possède des règles qui, par essence, sont très protectrices des données à caractère personnel (ci-après DAP). Le RGPD les présente et les organise différemment, mais nos obligations sont souvent déjà plus contraignantes.

Les considérants introductifs du RGPD démontrent une volonté de préserver au premier plan la place de l'humain et des valeurs morales, par exemple :

- *(2) (…) : Le présent règlement vise à contribuer à la réalisation d'un espace de liberté, de sécurité et de justice et d'une union économique, au progrès économique et social, à la consolidation et à la convergence des économies au sein du marché intérieur, ainsi qu'au bien-être des personnes physiques.*
- *(4) Le traitement des données à caractère personnel devrait être conçu pour servir l'humanité (…)*

C'est aussi le sens de notre serment et des principes essentiels de la profession.

Le RGPD n'est pas une contrainte nouvelle pour les avocats, mais, en définitive, une mise en perspective de règles que nous appliquons d'ores et déjà.

NB : avec le RGPD, l'obligation de déclaration des cabinets à la CNIL disparait. En contrepartie, il est attendu une responsabilisation des acteurs qui doivent être pro-actifs dans la mise en œuvre des protections.

Pour mémoire, le RGPD est entré en vigueur le 25/05/2018 : depuis cette date, les sanctions attachées au non-respect de la mise en œuvre sont encourues.

Attention : Le RGPD ne s'applique pas aux seules données clients mais à toute l'activité ; les collaborateurs et employés sont à la fois acteurs mais aussi personnes concernées ; le contrôle par les sous-traitants de leurs respect du RGPD doit également être contrôlé.

Ci-après des pistes de réflexions et de compréhension (plus que condensées) qui doivent contribuer à la mise en effectivité des obligations qui incombent aux cabinets, en les mettant en perspectives par rapport aux obligations auxquelles ils sont déjà soumises.

Droits garantis par le RGPD et mise en œuvre de leur effectivité :

1. droit d'accès	Délai d'un mois pour y répondre (+2 mois dans certains cas) : il s'agit du quotidien des cabinets – principe : gratuité (frais raisonnables selon les cas)
2. droit de rectification	Essence du travail du cabinet : avoir des informations à jour et utiles pour la défense des intérêts du client.
3. droit à l'effacement	Lorsque les données ne sont plus nécessaires au regard des finalités
4. droit à la limitation du traitement,	Les données sont isolées de façon à limiter leur traitement futur ou actuel
5. droit à la portabilité des données	La personne concernée peut les demander pour les conserver ou les transmettre à un autre service, même concurrent. Là encore, la profession a

	des règles établies et en particulier l'article 9.2 du RIN précise : « l'avocat dessaisi ne disposant d'aucun droit de rétention, doit transmettre sans délai tous les éléments nécessaires à l'entière connaissance du dossier ». *
6. droit d'opposition	A tout moment, sauf exception.
+ droit d'accès à l'autorité de contrôle	En France = la CNIL

Mise en œuvre des principes :

Principe de finalité	L'utilisation des données personnelles s'inscrit dans un objectif déterminé qui ne peut pas être détourné. La profession a déjà intégré cette obligation : le respect du mandat donné est la garantie de la profession. Le mandat est défini clairement dans la convention d'honoraire qui est désormais obligatoire.
Principe de proportionnalité et de minimisation des données	Seules les informations adéquates, pertinentes et nécessaires feront l'objet d'un TDAP. Là encore, la profession est en première ligne.
Principe d'une durée de conservation limité et droit à l'oubli	Exemples : Pour le judiciaire, la conservation des dossiers est désormais généralement de 5 ans à compter de la fin de la mission. Pour les collaborateurs et les employés : généralement, le temps de leur présence.
Principe de sécurité et de confidentialité	Seules les personnes autorisées peuvent avoir accès aux contenus et les contenus doivent être protégés ; là encore la déontologie nous oblige très précisément: code d'accès au téléphone, aux ordinateurs, pas de dossiers qui trainent dans la voiture ou dans la salle d'attente, pas de noms visibles, sécurisation des accès au cabinet, sécurisation des données informatiques, sécurisation des destructions d'archives… Pour mémoire, article 2 RIN (extraits) : * Le secret professionnel de l'avocat est d'ordre public. Il est général, absolu et illimité dans le temps. * L'avocat doit faire respecter le secret par les membres du personnel de son cabinet et par toute personne qui coopère avec lui dans son activité professionnelle. Il répond des violations du secret qui seraient ainsi commises. Pour mémoire, article 15.1 RIN (extrait) : L'avocat inscrit au tableau de l'Ordre doit disposer dans le ressort de son barreau d'un cabinet conforme aux usages et permettant l'exercice professionnel dans le respect des principes essentiels de la profession. Il doit aussi veiller au strict respect du secret professionnel et justifier d'une adresse électronique.
Principe du respect des droits des personnes	En ce sens que les personnes doivent avoir connaissance de leurs droits et de la façon dont elles peuvent les exercer : l'information doit être diffusée (site, convention, affichage…)

Obligations du responsable de traitement (avec ou sans délégué à la protection des données = DPO data privacy officer)

S'assurer que la finalité des traitements est définie	Encore une fois : cf. mandat et convention initiale
S'assurer que les dispositifs de sécurité et de confidentialité sont déterminés et respectés	Vérifier les accès, étudier les nécessités éventuelles (alarmes, sécurisation des ouvertures…). Vérifier la sécurisation des outils numériques (en particulier espaces cloud) …
S'assurer que les personnes concernées sont informées de leurs droits et les respecter	NB : les personnes concernées ne sont pas que les clients ; il peut s'agir des collaborateurs et des employés (exemple : pour dans le cadre d'un recrutement, il est interdit de relever le numéro de sécurité sociale = principe de minimisation)

S'assurer que les membres des cabinets et les sous-traitants respectent le RGPD	Sous-traitants à identifier : comptable, éditeur de logiciel, stockage en ligne, hébergeur… conclure un avenant au contrat si nécessaire.
Etablir un registre des activités de traitement	Quasi-obligatoire, simple et protecteur : faire une fiche par domaine (sous-traitant / dossiers clients éventuellement en distinguant juridique et judiciaire / employés / collaborateurs / vidéosurveillance / badges / site internet (NB : faire vérifier l'utilisation des cookies – Nota : il est rappelé que l'ouverture et la modification d'un site font l'objet d'une communication à l'ordre) / …
Etablir le cas échéant un code de bonne conduite	Pour rappeler les règles respectées / à respecter au sein du cabinet
Mentions obligatoires sur le site	Cf. fiche pratique CNB.
Notification auprès de la CNIL en cas de violation de données	NB la destruction / altération / divulgation qui peut entrainer un risque pour les droits et libertés des personnes doit être notifiée à la CNIL dans les 72 heures. Il existe un formulaire. Le process doit être connu et anticipé (exemple piratage)

Conclusion : pas de panique, il s'agit donc de matérialiser ce qui se fait déjà en vérifiant et en concrétisant les pratiques.

S'agissant des amendes encourues en cas de non-respect du RGPD, elles peuvent être colossales, mais, s'agissant pour la plupart également d'obligations déontologiques, elles pourraient aller de pair avec des sanctions déontologiques.

Pour finir, quitte à opérer cette mise à plat, en période de bonnes résolutions pour la rentrée, il peut être utile d'en profiter pour reprendre et vérifier :

- le calendrier de mise en conformité de l'accessibilité
- les mentions obligatoires sur les sites
- les mentions obligatoires pour les factures
- le modèle de convention d'honoraire

… en pensant à intégrer, quand nécessaire, les informations relatives au le RGPD et au médiateur.

VBD.

Liens utiles :

CNB : https://www.cnb.avocat.fr/fr/actualites/rgpd-telechargez-le-guide-pratique-elabore-pour-la-profession-davocat

LEXBASE : formation RGPD gratuite pour les avocats 2h - https://elearning.lexbase.fr/toutes-les-formations/14

CNIL : https://www.cnil.fr/fr/rgpd-en-pratique

CNIL : guide PME – avec explications - https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-guide-rgpd-tpe-pme.pdf

CNIL : texte du RGP - https://www.cnil.fr/fr/reglement-europeen-protection-donnees