



## La lettre juridique n°750 du 19 juillet 2018

[Avocats] Le point sur...

### L'impact du RGPD sur les cabinets d'avocats

N° Lexbase : N5041BXY



par Anne Renard, Directeur du département conformité et certification,  
Alain Bensoussan Avocats

**Le Règlement général sur la protection des données (RGPD) est entré en application il y a quelques semaines. S'il s'inscrit pleinement dans la continuité d'une réglementation qui date de 1978, force est de constater qu'un grand nombre de cabinets d'avocats peinent à se conformer aux exigences en résultant. Principale raison : les "robes noires" considèrent que le secret professionnel auquel ils sont astreints les dispense de se conformer au RGPD. Pourtant, c'est précisément pour cette raison qu'ils sont, au premier chef, concernés et doivent redoubler de vigilance. Décryptage.**

#### I – L'applicabilité du RGPD aux cabinets d'avocats

Le Règlement général sur la protection des données («RGPD» ou «GDPR» en anglais), adopté le 27 avril 2016, est applicable dans l'ensemble des Etats membres de l'Union européenne depuis le 25 mai 2018 [1].

Il s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services à des résidents européens. En pratique, il s'applique donc chaque fois qu'un résident européen sera directement visé par un traitement de données [2].

Dès lors que les cabinets d'avocats mettent en œuvre des traitements de données à caractère personnel, en particulier dans le cadre de la gestion de leurs clients, ils sont tous concernés, peu importe leur taille ou leur structure d'exercice.

Les traitements des données des clients ne sont d'ailleurs pas les seuls concernés. Tous les traitements liés à la gestion des ressources humaines, à la sollicitation personnalisée, à la communication externe, à la gestion de leur comptabilité, à la surveillance des locaux (vidéosurveillance ou badge par exemple) constituent des traitements de données à caractère personnel soumis au nouveau règlement.

## II – Les principales obligations des cabinets d'avocats

**Principe d 'accountability.** Avec l'entrée en vigueur du RGPD, les avocats doivent adopter une véritable posture Informatique et Libertés. Le RGPD impose de manière générale aux cabinets d'avocats de se soumettre à de nouvelles obligations, dont celle d'être en mesure de démontrer, à tout moment, la conformité de leurs traitements (principe de responsabilisation ou d' *accountability*).

**Qualité des données.** Les données doivent être collectées de manière loyale et licite et pour une finalité déterminée, explicite et légitime. Elles doivent, en outre, être adéquates, pertinentes et limitées à ce qui est nécessaire. Avant de mettre un œuvre un traitement des données à caractère personnel, il conviendra de s'interroger sur la nécessité de traiter ces données et, dans la mesure où un tel traitement s'avère indispensable, sur les données qui permettront d'atteindre les finalités recherchées par le traitement [3].

**Durée de conservation.** Ces données ne doivent par ailleurs pas être conservées au-delà de la durée nécessaire aux finalités pour lesquelles elles ont été collectées [4]. Bien souvent, aucune véritable politique de durée de conservation n'est mise en œuvre au sein des cabinets, à l'exception du recours à un archivage papier. Les données ne peuvent être conservées de manière illimitée et l'avocat ne saurait être le tiers archiveur de son client. Le respect de ce principe implique la mise en place, au sein des cabinets d'avocats, d'une politique de durée de conservation et de purge tant pour les supports papiers que pour les supports numériques.

**Mentions et contrats.** La conformité au RGPD passe également par l'information des personnes concernées [5]. Cette information peut se faire par le biais de mentions particulières au sein des conventions d'honoraires, sur le site *web* ou les formulaires de collecte des données utilisés au sein du cabinet.

Par ailleurs, les avocats, en tant que responsables du traitement, doivent prêter une attention particulière aux contrats de sous-traitance conclus avec les prestataires auxquels ils recourent : prestataires informatiques, éditeurs de logiciel, ou encore prestataires en charge la paie. Conformément aux exigences du RGPD, les cabinets d'avocats devront mettre en place un contrat ou acte juridique avec leurs sous-traitants comportant un certain nombre de mentions spécifiques relatives à la protection et confidentialité des données et aux droits et obligations des parties dans le cadre des traitements mis en œuvre [6].

**Sécurité et violation des données.** Dès lors que, parmi les données collectées par les cabinets d'avocats, figurent des catégories particulières de données ou des données relatives à des infractions ou condamnation pénale, il est essentiel de mettre en œuvre des mesures de sécurité, tant logique que physique, qui soient adaptées aux risques présentés par ce type de traitements. Ceci est d'autant plus important que le RGPD instaure l'obligation de notifier à la Cnil toute violation de données à caractère personnel et, en cas de risque élevé pour les droits et libertés des personnes concernées, l'obligation de communiquer sur l'existence d'une telle violation de sécurité auprès de ces personnes. La publicité d'une telle violation serait particulièrement préjudiciable pour l'image d'un cabinet.

**Droits des personnes.** Par ailleurs, il convient d'être en mesure non seulement d'informer les personnes concernées mais aussi de répondre à l'ensemble de leurs demandes d'exercice de droit (droit d'accès, droit à l'effacement droit à la portabilité, etc.) étant précisé que les cabinets d'avocats ne disposent que d'un mois pour répondre à une telle demande. Ce délai peut être prolongé à deux mois, compte tenu de la complexité et du nombre des demandes [7].

**Flux transfrontières.** Certains cabinets d'avocats sont amenés à transférer des données à caractère personnel en

dehors de l'Union européenne, et notamment les cabinets appartenant à des structures internationales. Or, dans ce cas, il est bien souvent nécessaire de prendre des garanties appropriées comme, par exemple, en concluant des clauses contractuelles types afin de s'assurer que le niveau de protection des données soit suffisant. Il est également nécessaire d'informer les personnes concernées sur l'existence de tels flux.

**Délégué à la protection des données.** Le Règlement général sur la protection des données impose de désigner un délégué à la protection des données (ou DPO) notamment lorsque l'activité, cœur de métier du responsable de traitement ou sous-traitant, requiert le suivi régulier et systématique de données à une large échelle ou lorsque l'activité cœur de métier du responsable ou du sous-traitant consiste à traiter à une large échelle des données sensibles ou relatives à des condamnations ou infractions. A cet égard, il est important de relever que le considérant g1 du RGPD précise que le traitement de données à caractère personnel de clients par un avocat exerçant à titre individuel ne devrait pas être considéré comme constituant un traitement à grande échelle. Au regard de ces critères, il semble que la majorité des cabinets d'avocats n'a pas à désigner de DPO. Toutefois, en fonction de la taille et du secteur d'activité du cabinet d'avocat, une telle désignation doit en tout état de cause s'analyser en opportunité dans la mesure où elle permettrait de désigner une personne afin d'accompagner le cabinet dans sa mise en conformité.

**Registre des traitements.** Le responsable de traitement doit tenir un registre relatif aux traitements de données mises en œuvre sous sa responsabilité. Cette obligation ne s'impose pas aux entreprises comptant moins de 250 salariés, sauf si le traitement qu'elles effectuent est susceptible de comporter un risque au regard des droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur des données sensibles ou sur des données se rapportant à des condamnations et des infractions pénales. Au regard de ces critères, les cabinets d'avocats semblent tenus de devoir mettre en place un tel registre et une cartographie préalable des traitements mis en œuvre au sein du cabinet est nécessaire pour pouvoir remplir une telle obligation.

**Analyse d'impact.** Le RGPD [8] prévoit encore que lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement doit effectuer, avant toute mise en œuvre, une analyse d'impact. A cet égard, et notamment en raison des termes du considérant g1 du RGPD (cf. *supra*), il semblerait que les cabinets d'avocats seront peu concernés par cette obligation. Néanmoins, un cabinet d'avocats, quel que soit sa taille, pourrait être amené à réaliser des analyses d'impact si les traitements mis en œuvre répondent à certaines caractéristiques.

### III – L'avocat : responsable de traitement ou sous-traitant ?

Les cabinets reçoivent de plus en plus de demandes, de la part de leurs clients, de justifier de leur conformité au RGPD. Et pourtant, le seul fait que le cabinet d'avocats soit mandaté par son client ne présume pas de sa qualité de sous-traitant.

Concernant l'avocat plaçant, la Cnil considère que « *dans le cadre de la gestion des affaires contentieuses, les avocats agissent en qualité de responsable de traitement* » [9]. En effet, celui-ci agit en toute indépendance dans l'exercice de sa mission et met en œuvre des traitements de données à caractère personnel qui sont accessoires pour réaliser sa mission à la demande du client. Il ne reçoit pas d'instruction de la part du client pour la réalisation même du traitement de données à caractère personnel. Le Groupe de travail « article 29 » était lui aussi venu préciser qu'un avocat pouvait être qualifié de responsable de traitement dès lors qu'il jouait, dans sa mission d'expertise, un rôle prépondérant [10].

Concernant l'avocat conseil, il n'est pas toujours amené à traiter des données à caractère personnel. En pratique, lorsque l'avocat a accès à un certain nombre de données personnelles dans le cadre de sa mission de conseil, il devrait également être qualifié de responsable de traitement. Toutefois, la Cnil a pu considérer que l'avocat, intervenant dans un audit sur la « *base d'instructions strictement définies par leurs clients* » [11], pourrait se prévaloir de la qualité de sous-traitant.

Il convient d'ajouter que l'Information Commissioner's Office s'est également très récemment prononcée en faveur de la responsabilité de traitement en considérant qu'en fonction de son implication et du détachement des instructions du client, l'avocat peut être considéré comme un responsable de traitement [12].

#### IV — La protection du secret professionnel de l'avocat

On l'a dit, nombre d'avocats invoquent le secret professionnel auquel ils sont soumis pour être dispensés de se conformer aux obligations découlant du RGPD. Or, il ne fait aucun doute que nous sommes pleinement soumis à cette réglementation, et probablement encore plus à raison de la garantie de ce secret professionnel dont nous sommes investis.

Le RGPD et la loi Informatique et libertés, telle que modifiée par la loi relative à la protection des données personnelles (LXBL7645LKD), prévoient un certain nombre d'exceptions pour qu'il n'y ait pas d'entrave au secret professionnel de l'avocat ce qui, *a fortiori*, démontre bien que l'avocat est pleinement soumis à cette réglementation.

Néanmoins, lors d'un contrôle par la Cnil, le secret ne peut lui être opposé que lorsque les informations sont couvertes par le secret professionnel « applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou [...] par le secret médical » [13]. Les informations sortant du champ de protection du secret professionnel, seront donc susceptibles d'être contrôlées par la Cnil. Sont concernées notamment les données à caractère personnel des collaborateurs et des salariés du cabinet par exemple.

On le voit, la mise en conformité avec le RGPD est un enjeu majeur pour toutes les entreprises, en ce incluant les cabinets d'avocats. Les responsables de traitement et les sous-traitants peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du RGPD. Les amendes administratives peuvent s'élever jusqu'à 10 ou 20 millions d'euros, ou, dans le cas d'un cabinet d'avocats, de 2 % jusqu'à 4 % du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

La mise en conformité des cabinets d'avocats est une nécessité et, outre le gage de confiance qu'elle constitue pour les clients et les collaborateurs, elle risque fort de devenir un enjeu de positionnement concurrentiel entre les cabinets d'avocats eux-mêmes face aux entreprises qu'elles accompagnent.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (N° Lexbase : L018gK8I).

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, art. 3

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, art. 5

[4] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, art. 5.

[5] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, art. 13 et art. 14.

[6] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, art. 28.

[7] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, art. 12 (3)

[8] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, art. 35.

[9] Cnil, Guide « Les avocats et la loi Informatique et libertés », 2011 (cf. l'Encyclopédie "La profession d'avocat" N° Lexbase : E9540ETI).

[10] G29, Avis 1/2010, sur les notions de « responsable du traitement » et de « sous-traitant ».

[11] Cnil, Guide « *Les avocats et la loi Informatique et libertés* », 2011.

[12] ICO, *Data controllers and data processors : what the difference is and what the governance implications are*, p. 9.

[13] Loi n° 2018-493 du 20 juin 2018, relative à la protection des données personnelles (N° Lexbase : L7645LKD).