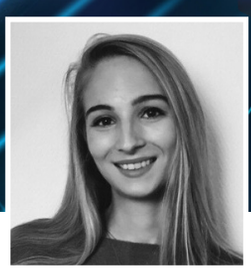
La digitalisation des cabinets d'avocats : pourquoi se sentir concerné par la protection des données et la sécurité de l'information ?



Audrey Malaise
Consultante en protection des données personnelles chez CRANIUM

Solène Navet
Consultante en protection des données personnelles chez CRANIUM

De nos jours, rares sont les aspects de nos vies qui échappent encore à la digitalisation de l'information. Ce processus, défini par le dictionnaire Larousse comme un « processus de transformation des services (financiers, commerciaux) d'une entreprise, par un recours accru aux technologies de l'information », n'a pas épargné les cabinets d'avocats. Que ce soit par la numérisation des documents, l'utilisation de logiciels de gestion des dossiers ou encore le recours à des bases de données en ligne, même les avocats les plus réticents digitalisent leur pratique.

Si la digitalisation présente de nombreux avantages, tels que la réduction de la quantité de papier à produire, stocker et manipuler, une plus grande praticité dans les recherches, une augmentation de la productivité, etc., elle comporte également des risques. L'utilisation de logiciels, surtout dans le *cloud*, implique généralement la transmission de données à une partie tierce et, dès lors, une perte de contrôle sur les données traitées et la protection qui leur est accordée. Cette perte de contrôle représente un risque tant au niveau de la protection de la vie privée que de la sécurité de l'information.

– INNOVATION –

En décidant de digitaliser leur pratique, les avocats doivent donc être vigilants à mettre en place des mesures appropriées pour la sécurité de leurs informations ainsi que s'assurer du respect de la législation relative à la protection des données à caractère personnel.

LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL AU SEIN D'UN CABINET D'AVOCATS

Les avocats sont amenés à traiter de nombreuses données personnelles, y compris des données dites sensibles ou judiciaires, dans le cadre de leur activité. L'avocat doit donc veiller à respecter les obligations qui lui incombent en vertu de la législation sur la protection des données à caractère personnel, tout en les conciliant avec les règles de déontologie et le secret professionnel de l'avocat.

Bien que le champ d'application matériel du Règlement Général sur la Protection des Données (ci-après « le RGPD »), couvre également le traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, le cadre réglementaire de la protection des données est particulièrement important dans un contexte digital puisqu'il permet de maîtriser les données à caractère personnel traitées et d'en conserver le contrôle. Cet article vous présente, de manière pratique, les différents points à prendre en considération pour la mise en conformité de votre cabinet.

1_Rôles et responsabilités

L'article 37 du RGPD prévoit les cas dans lesquels la nomination d'un Délégué à la Protection des Données (Data Protection Officer en anglais, DPO en abrégé) est obligatoire. Il serait erroné de dire qu'elle est obligatoire dans les cabinets d'avocats, l'analyse devant se faire au cas par cas, en tenant compte du type de données à caractère personnel traitées et de leur quantité. Ainsi, selon les matières pratiquées, il sera plus ou moins indiqué de nommer un DPO. Par exemple, les cabinets d'avocat pratiquant le droit médical seront amenés à traiter des données sensibles, ce qui ne sera pas forcément le cas en droit des sociétés.

Pour autant, même si la nomination d'un DPO n'est pas obligatoire, cela ne dispense pas le cabinet de sa responsabilité au regard du RGPD. Les cabinets d'avocats doivent établir un plan d'actions concret, avec des délais et des personnes en charge de la réalisation des actions, pour démontrer le processus de mise en conformité.

2_Sensibilisation et communication

Dans un processus de mise en conformité, le DPO n'est pas le seul acteur. Tous les collaborateurs et employés d'un cabinet d'avocats doivent être conscientisés afin qu'ils participent, au quotidien, au respect des règles du RGPD en implémentant les bonnes pratiques. Il relève de la responsabilité du cabinet de communiquer sur la protection des données et d'organiser des activités de sensibilisation spécifiques pour accroître les connaissances du RGPD des différents acteurs.

3_Registre des activités de traitement

Le RGPD, en son article 30, prévoit une obligation, pour tout responsable de traitement et tout sous-traitant de données personnelles, de maintenir un registre des activités de traitement. Ce registre, qui doit être accompagné d'une procédure organisant sa mise à jour, doit contenir des champs prévus directement dans le RGPD. Au-delà des champs obligatoires, il est recommandé d'ajouter d'autres champs tels que la base de licéité ou la localisation des données afin de faciliter l'exercice des droits des personnes concernées. Cela permet également, en cas de contrôle par une autorité de supervision, de démon-

trer un certain niveau de maturité et un contrôle sur les données à caractère personnel traitées.

Il est à noter qu'il existe une exemption à la tenue d'un tel registre pour les entreprises ou organisations de moins de 250 employés, sauf si le traitement est susceptible d'entraîner un risque pour les droits et libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte sur des données sensibles et judiciaires. Toutefois, compte tenu des conditions strictes d'application de l'exemption, sa portée est très limitée et il est peu probable qu'elle puisse être invoquée par des avocats.

4_Droits de la personne concernée

Les droits des personnes concernées constituent une priorité dans la mise en conformité d'une entreprise quelle qu'elle soit. En effet, cet aspect de la réglementation est le plus facile à contrôler puisque tout individu concerné peut demander à exercer ses droits. Si ces droits ne sont pas respectés, la personne concernée peut facilement introduire une plainte auprès de l'autorité de supervision qui pourra alors mener une enquête. Afin d'éviter une investigation en profondeur, il est donc primordial de permettre aux personnes concernées d'exercer leurs droits.

Une conformité sur ce point nécessite une procédure pratique qui doit être communiquée à toutes les personnes concernées dans l'organisation. Cette procédure doit reprendre l'ensemble des étapes : la manière dont les personnes concernées peuvent introduire leur demande d'exercice, la manière dont l'organisation reçoit et accuse réception de la demande, la manière dont l'identité du demandeur est vérifiée, la méthodologie de gestion de la demande, etc. À l'instar des autres blocs du RGPD, il faut pouvoir documenter les mesures prises pour assurer le respect de ces prescriptions.

Les personnes concernées ont notamment le droit d'être informées sur les traitements de leurs données personnelles effectués par votre cabinet d'avocats et, dans certains cas, la seule possibilité pour que le traitement de données soit légal est de demander le consentement de la personne concernée. Des mécanismes de transparence et de collecte de consentement doivent donc être mis en place au sein du cabinet. Cela concerne également le site web de votre cabinet d'avocats, surtout lorsque des cookies autres que fonctionnels y sont utilisés.

« Les droits des personnes concernées constituent une priorité dans la mise en conformité d'une entreprise quelle qu'elle soit »

5_Relations avec les tiers

De manière générale, le RGPD impose d'avoir une bonne vue d'ensemble sur les relations entretenues avec des tiers, quand des données personnelles sont impliquées. Des registres, tenus à jour, reprenant les tiers et leur rôle du point de vue de la protection des données peuvent aider à la conformité. Au sens du RGPD, un destinataire est considéré comme étant une personne physique, morale, une autorité publique, un service ou tout autre organisme qui reçoit communication des données à caractère personnel, qu'il s'agisse ou non d'un tiers. Un responsable distinct pour lequel votre cabinet n'agit pas en tant que sous-traitant et qui agit pour ses propres finalités est dès lors être considéré comme un destinataire. Il en va de même pour les autorités auxquelles il convient d'envoyer certaines données personnelles, par exemple la police ou les tribunaux.

Le RGPD n'exige pas la conclusion d'accord spécifique avec les destinataires de données, sauf si ces destinataires ont la qualité de sous-traitants ou responsables conjoints. De tels accords ne sont donc en théorie pas obligatoires, cependant, il est toujours préférable de conclure des accords de partage de données. Toutefois, comme mentionné précédemment, pour les tiers qui sont sous-traitants ou responsables conjoints, il faut s'assurer d'avoir conclu des accords contractuels conformes au RGPD avec ces parties.

Il est également important de choisir des partenaires, des sous-traitants qui assurent un niveau élevé de protection des données, il en va de la responsabilité du cabinet d'avocats en tant que responsable du traitement. Pour s'assurer de n'oublier aucune étape et de ne négliger aucun aspect dans le processus de sélection de sous-traitants, une politique de sélection des sous-traitants peut être mise sur pied et il faut toujours avoir à disposition un modèle d'accord de sous-traitance.

« Il est également important de choisir des partenaires, des sous-traitants qui assurent un niveau élevé de protection des données »

6_Transferts internationaux

Depuis l'arrêt Schrems II, les transferts internationaux constituent un sujet brûlant. Il convient de répertorier les transferts de données en dehors de l'Espace économique européen effectués par le cabinet. Ces transferts peuvent être identifiés grâce au registre des activités de traitement. Afin de pouvoir poursuivre ces transferts de données, souvent nécessaires à l'utilisation de certains services ou logiciels, il faut évaluer leur impact au travers d'un *Transfer Impact Assessment*. Ces analyses permettent d'identifier le besoin de mesures complémentaires dans les cas où l'utilisation des mécanismes de garanties énumérés par le RGPD ne suffit pas.

7_Gestion des violations de données

Le RGPD oblige les responsables de traitement à adopter certains comportements en cas de violation de données à caractère personnel. Les cabinets d'avocats n'échappant pas à la règle, il convient de mettre en place une procédure de détection et de gestion de ces incidents, et de former le personnel à l'application d'une telle procédure. En effet, les collaborateurs et employés d'un cabinet d'avocats sont en première ligne pour détecter les violations de données. Il est donc important qu'ils adoptent les bons réflexes dans ces situations.

Par ailleurs, la procédure doit prévoir les cas où l'Autorité de protection des données et/ou les personnes concernées doivent être notifiées. Il est souvent préférable de notifier l'Autorité de protection des données en cas de doute car cela démontre un certain niveau de maturité du cabinet. Toutes ces violations et le suivi qui leur est accordé doivent être consignés dans un registre des violations de données.

8_Analyses d'impact sur la protection des données

Depuis l'entrée en vigueur du RGPD, les notions de « protection des données dès la conception et protection des données par défaut » obligent les institutions à considérer la protection des données à caractère personnel dès les prémisses d'un nouveau traitement de données, d'un nouveau

«La sécurité des données est au cœur du RGPD »

projet ou de l'acquisition d'un nouveau logiciel. Dans certains cas, le responsable de traitement est obligé de formaliser l'exercice en réalisant une analyse d'impact sur la protection des données (AIPD).

Si le traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques, le responsable de traitement doit mener une analyse d'impact en suivant la procédure qu'il aura préalablement prévue.

LA SÉCURITÉ DE L'INFORMATION AU SEIN D'UN CABINET D'AVOCATS

La sécurité des données est au cœur du RGPD. Cependant, c'est souvent l'aspect le plus compliqué à appréhender pour des spécialistes du droit qui n'ont pas de connaissances approfondies en matière de sécurité de l'information (au sens large). Pour autant, la digitalisation des données amène de nouveaux risques en matière de violations de données ou de cyberattaques.

Au cours des dernières années, plusieurs cabinets d'avocats ont été ciblés par des cyberattaques en raison de la valeur des données qu'ils traitent. Des répercussions graves peuvent résulter de ce type d'actes malveillants. Plusieurs raisons peuvent expliquer l'attrait grandissant des cybercriminels pour les cabinets d'avocats : la possibilité de voler l'identité de dirigeants ou décideurs, la possibilité de fraude financière, la possibilité de commettre des délits d'initiés, etc.

1_Faire le point sur la situation du cabinet

Lorsqu'un cabinet d'avocats décide d'améliorer sa gestion de la sécurité de ses informations, il convient tout d'abord de dresser un état des lieux de la situation. Il est important de connaître ses ressources en termes d'information pour pouvoir ensuite les protéger adéquatement : données à caractère personnel, informations confidentielles sur le client, données personnelles sensibles, dossiers des clients, dossiers du personnel, budgets, stratégies pour les procédures judiciaires, finances, contrats, etc.

Dans un second temps, il faut pouvoir localiser ces données. L'endroit où sont stockées les données peut être physique ou digital. Dans les deux cas, une connaissance précise du lieu où trouver les informations servira de base pour leur sécurisation. En effet, en fonction de la méthode et du lieu de stockage choisi par le cabinet, les mesures de sécurité ne seront pas les mêmes.

2_Mesures d'atténuation des risques

En dehors des certifications et standards internationalement reconnus, il existe de nombreuses mesures qui peuvent être prises, dépendant du niveau de risque et de la valeur de l'information, pour atténuer les risques d'atteinte à la sécurité de l'information.

Ces quelques mesures de base doivent être communiquées au sein de l'organisation afin de sensibiliser l'ensemble du personnel et en faire des réflexes du quotidien. Il s'agit par exemple de former le personnel à reconnaître des tentatives de phishing ou d'ingénierie sociale. Une bonne gestion des mots de passe est également importante. En utilisant l'authentification multifactorielle et en imposant un changement régulier des mots de passe ainsi qu'une certaine complexité de ceux-ci, le risque d'accès indésiré est déjà fortement réduit.

D'autres mesures simples existent : toujours accompagner les visiteurs, utiliser un VPN, mettre en place une politique de bureau propre, ne pas utiliser le WIFI public gratuit, séparer les communications professionnelles et personnelles, etc.

3_Normes applicables à la sécurité de l'information

Au-delà de ces mesures simples, il existe différentes normes qui peuvent être mises en place pour assurer un niveau élevé de sécurité de l'information. Ces standards, tels que le standard ISO 27001, proposent une méthode structurée de sécurisation de l'information. Ces normes, qui prennent en compte le respect du RGPD, constituent un excellent moyen d'assurer que vos ressources en termes d'information sont en sécurité.