CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

AVOCATS
BARREAU
• PARIS

Conférence des Bâtonniers

GUIDE PRATIQUE

LES AVOCATS ET LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES (RGPD)

1re ÉDITION

CONSEIL NATIONAL DES BARREAUX
BARREAU DE PARIS
CONFÉRENCE DES BÂTONNIERS

MARS 2018

TABLE DES MATIÈRES

AVANT-PROPOS 5

CADRE GÉNÉRAL DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL 7

1. La protection des données personnelles, un enjeu particulièrement sensible pour les avocats 7
2. Glossaire 8
3. Les principes clés 9

3.1. Principes réaffirmés 9

3.1.1. Le principe de finalité : une utilisation encadrée des données à caractère personnel 9
3.1.2. Le principe de proportionnalité 9
3.1.3. Le principe d'une durée de conservation limitée des données 9
3.1.4. Les principes de sécurité et de confidentialité 10
3.1.5. Le principe du respect des droits des personnes 10

3.2. Nouvelles mesures de conformité 12

3.2.1. Notification de toute violation de données à caractère personnel 13
3.2.2. Minimisation des données 13
3.2.3. Droit à l'oubli 13
3.2.4. Analyses d'impact 14
3.2.5. Portabilité des données 14
3.2.6. Capacité à suivre les destinataires de données à caractère personnel 16
3.2.7. Tenue d'un registre des activités de traitement 16

FICHES PRATIQUES 17

FICHE N°1. LE TRAITEMENT « RH » (RESSOURCES HUMAINES) 18

1. Qu'est-ce qu'un traitement RH ? 18
2. Quelles sont les données que l'avocat peut collecter dans le cadre d'un traitement RH ? 18
3. L'avocat doit-il procéder à des formalités en cas de traitement RH ? 19
4. Combien de temps les données peuvent-elles être conservées ? 20
5. Doit-il y avoir une information des personnes concernées ? 20

FICHE N°2. GESTION DES CLIENTS 22

1. Quelles données l'avocat peut-il collecter dans le cadre de la gestion de ses clients ? 22
2. L'avocat doit-il procéder à des formalités ? 23
3. Combien de temps les données peuvent-elles être conservées ? 24
4. Doit-il y avoir une information des personnes concernées ? 24
5. La sécurité des dossiers clients 25
6. Sollicitation personnalisée 25

FICHE N°3. VIDÉOSURVEILLANCE ET VIDEOPROTECTION 26

1. Qu'est-ce que la vidéosurveillance et la vidéoprotection ? 26
2. Quel est l'objectif de l'installation de caméras ? 26
3. Quelles sont les formalités à accomplir ? 27
   - **3.1.** Avant l'entrée en vigueur du RGPD 27
   - **3.2.** Après l'entrée en vigueur du RGPD 27
4. Est-il nécessaire d'informer les personnes concernées ? 28
5. Qui peut accéder aux images des caméras ? 28
6. Combien de temps les images peuvent-elles être conservées ? 29

FICHE N°4. FOURNISSEURS ET PRESTATAIRES 30

1. Qu'est-ce qu'un sous-traitant ? 30
2. Que faire en cas de sous-traitance ? 30
3. Que faire avec les sous-traitants avec lesquels le cabinet est déjà en relation commerciale ? 31

FICHE N°5. LA GESTION DES ACCES AU CABINET 31

1. L'utilisation de badges sur le lieu de travail 32
2. Les dispositifs biométriques 33

FICHE N°6. LA LUTTE CONTRE LE BLANCHIMENT ET LE FINANCEMENT DU TERRORISME 34

FICHE N°7. SITES INTERNET 36

1. Quelles sont les formalités à accomplir si l'avocat collecte des données à caractère personnel via son site internet ? 36
2. Quelles sont les mentions qui doivent être obligatoirement présentes sur le site Internet de l'avocat ? 37
3. Que doivent contenir les différentes mentions ? 37
4. Qu'est-ce qu'un cookie ? 39
5. Comment rendre conforme l'utilisation des cookies sur le site Internet de l'avocat ? 39

FICHE N°8. BONNES PRATIQUES DE SECURITE DES DONNEES 41

1. Pourquoi la sécurité des données à caractère personnel est particulièrement importante dans les traitements opérés par l'avocat ? 41
2. Quelles mesures de sécurité physiques dois-je mettre en place ? 41
3. Quelles mesures de sécurité logiques/numériques dois-je mettre en place ? 41
4. Comment notifier et communiquer sur une violation des données à caractère personnel ? 42

FICHE N°9. PROCEDURE EN CAS DE VIOLATION DE DONNEES 43

FICHE N°10. LE REGISTRE DES ACTIVITES DE TRAITEMENT 45

FICHE N°11. LE DELEGUE À LA PROTECTION DES DONNEES 47

1. Obligation des cabinets d'avocats de désigner un délégué à la protection des données 47
2. Obligations et missions du délégué à la protection des données 48
3. Avocat agissant en qualité de délégué à la protection des données 49

FICHE N°12. AUTORITE DE CONTROLE ET SANCTIONS 51

FICHE N°13. DROIT D'ACCES AUX DONNEES 52

MÉTHODOLOGIE DE MISE EN CONFORMITÉ 54

1. La désignation d'un pilote 54
2. La cartographie des traitements de données personnelles 54
3. Identifier les actions prioritaires 56
4. La gestion des risques 56
5. La mise en place de processus de protection de données personnelles au sein du cabinet d'avocats 56
6. La documentation de la conformité 57

POUR EN SAVOIR PLUS 58

AVANT-PROPOS

Le Règlement (UE) 2016/679 relatif à la protection des données (RGPD) sera directement applicable dans l'ensemble des Etats membres le 25 mai 2018.

Il reste deux mois aux cabinets d'avocats pour anticiper ce nouveau texte qui va modifier en profondeur les règles applicables à leur environnement digital.

Le traitement des données à caractère personnel des clients du cabinet d'avocats est particulièrement sensible. Il obéit à une logique spécifique, qui n'est pas celle d'une entreprise purement commerciale : la protection des données sensibles dont il a connaissance est inhérente au lien de confiance unissant l'avocat à son client et au respect de ses obligations déontologiques.

Le Conseil national des barreaux, le Barreau de Paris et la Conférence des bâtonniers sont aux côtés des avocats pour les accompagner dans la mise en conformité au RGPD, la sécurisation de leurs données et celles de leurs clients.

Ce guide pratique apporte des réponses concrètes aux questions des avocats et leur permettra de jouer un rôle essentiel en matière de protection des données et de la vie privée, tant comme responsable de traitement que comme conseil auprès de leurs clients.

En effet, le RGPD est non seulement de nature à renforcer la confiance et la sécurité nécessaires dans les relations avec les clients, mais aussi une formidable opportunité pour les avocats d'investir un nouveau champ d'intervention auprès de leurs clients.

L'avocat apparaît comme un technicien du droit particulièrement compétent pour aider ses clients à se mettre en conformité avec le RGPD et exercer la fonction de délégué à la protection des données. Bien que les avocats CIL soient encore peu nombreux, l'avocat a pleinement sa place dans ce marché qui s'ouvre aujourd'hui dans un très grand nombre d'entreprises. Cette nouvelle fonction permet à la profession d'élargir naturellement son offre de services et de conseils, inscrivant sa relation avec le client dans une perspective durable et *full service* dans le strict respect de nos règles professionnelles.

Les nombreuses recommandations contenues dans ce guide doivent permettre aux avocats d'occuper une place toujours plus importante dans ce domaine du droit.

Christiane Féral-Schuhl,
présidente du Conseil national des barreaux

Marie-Aimée Peyron,
vice-présidente du Conseil national des barreaux, Bâtonnier du Barreau de Paris

Jérôme Gavaudan,
vice-président du Conseil national des barreaux, président de la Conférence des Bâtonniers

CADRE GÉNÉRAL DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

CADRE GÉNÉRAL DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Le règlement n° 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 des données (règlement général sur la protection des données – RGPD) entre en vigueur le 25 mai 2018. Il abroge la directive 95/46/CE.

Le RGPD est une règlementation européenne obligatoire qui refond et renforce les droits et la protection des données à caractère personnel des personnes physiques.

Le RGPD s'applique à tous les cabinets d'avocats, quelle que soit leur taille, leur structure et leur domaine d'activité.

1. La protection des données personnelles, un enjeu particulièrement sensible pour les avocats

Les données auxquelles l'avocat a accès dans l'exercice de ses fonctions relèvent très souvent de la vie privée de leurs clients et sont par nature très sensibles : données relatives à la santé, casier judiciaire, opinions politiques et religieuses, situation familiale, etc...

Leur divulgation peut porter atteinte aux droits et libertés des personnes concernées. Les informations traitées par les avocats pour l'exercice de leur profession doivent être protégées de manière particulière.

Le respect du secret professionnel, tel que défini par l'article 66-5 de la loi du 31 décembre 1971, l'article 4 du décret du 12 juillet 2005, l'article 2 du Règlement intérieur national (RIN) et protégé par l'article 226-13 du code pénal, doit conduire l'avocat à être particulièrement vigilant à l'égard de la protection des données à caractère personnel de ses clients et, par conséquent, à se conformer aux obligations légales et règlementaires applicables en la matière.

Protéger les données à caractère personnel de son client est essentiel pour garantir le secret professionnel.

Le respect par les avocats des règles de protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard de ses clients.

C'est également un gage de sécurité juridique pour les avocats eux-mêmes qui, responsables des traitements mis en œuvre, doivent notamment veiller à ce que :

- la finalité de chacun des traitements et les éventuelles transmissions d'informations sont clairement définies ;
- les dispositifs de sécurité informatiques et physiques sont précisément déterminés ;
- les mesures d'information des personnes concernées sont appliquées.

Le traitement des données à caractère personnel des clients du cabinet d'avocats est particulièrement sensible. Il obéit à une logique spécifique, qui n'est pas celle d'une entreprise purement commerciale : la protection des données sensibles dont il a connaissance est inhérente au lien de confiance unissant l'avocat à son client et au respect de ses obligations déontologiques.

Si le croisement des nouvelles technologies et de la déontologie peut apparaître délicat, il convient d'avoir à l'esprit un principe simple : l'avocat est, en toutes circonstances, tenu de respecter les règles déontologiques. En d'autres termes, l'évolution des modalités pratiques d'exercice de la profession induite par les nouvelles technologies que chaque avocat met en œuvre au sein de son cabinet ne peut l'affranchir, ni du respect des dispositions du Règlement intérieur national (RIN), ni du règlement intérieur de chaque barreau, ni de l'obligation de faire respecter ces règles par l'ensemble des membres de son cabinet et par les prestataires extérieurs auxquels il fait appel pour les besoins de son activité.

Cette règle impérative concerne aussi bien l'externalisation de certains services du cabinet (standard déporté, secrétariat à distance, traducteur, etc.), que l'externalisation de l'hébergement des données du cabinet (Cloud Computing) ou de l'exploitation de ses outils de communication (site Internet, blog, sites de référencement, site tiers, consultation en ligne, etc.).

C'est par ce souci constant du respect de leurs obligations déontologiques dans l'univers du numérique, et en assurant particulièrement la protection des données du cabinet et du respect du secret professionnel, que les avocats pourront serainement prendre le virage du numérique sans perdre leur valeur et la confiance de leurs clients.

L 'avocat, garant du secret professionnel, clé de voûte de la profession, se doit d'être particulièrement exemplaire en la matière.

2. Glossaire

- **Données à caractère personnel :** toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.
- **Traitement :** toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
- **Responsable du traitement :** la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

- **Sous-traitant :** la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
- **Destinataire :** la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

3. Les principes clés

Le RGPD vient réaffirmer des principes essentiels en vigueur sous l'empire de la Directive 95/46. Des mesures nouvelles de conformité ont en outre été introduites.

3.1. Principes réaffirmés

3.1.1. Le principe de finalité : une utilisation encadrée des données à caractère personnel

Les données à caractère personnel ne peuvent être recueillies et traitées que pour une finalité déterminée explicite et légitime, correspondant aux objectifs poursuivis par l'avocat responsable du traitement.

Ainsi, à titre illustratif, lorsqu'il accède au serveur professionnel des données cadastrales de la direction générale des impôts, un avocat ne doit pas porter atteinte à la vie privée de la personne concernée par ces informations, notamment en utilisant ces informations à des fins de prospection commerciale, de démarchage politique ou électoral.

Tout détournement de finalité est passible de 5 ans d'emprisonnement et de 300 000 euros d'amende (article 226-21 du code pénal).

3.1.2. Le principe de proportionnalité

Seules les informations adéquates, pertinentes et nécessaires à la finalité du traitement peuvent faire l'objet d'un traitement de données à caractère personnel.

Par exemple, il n'est pas utile d'enregistrer des informations sur l'entourage familial d'une personne lorsque, au regard des finalités d'un traitement et de la nature de l'affaire traitée, seuls sont nécessaires des éléments relatifs à sa vie professionnelle.

3.1.3. Le principe d'une durée de conservation limitée des données

Les informations figurant dans un fichier ne peuvent être conservées indéfiniment. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier.

Les enregistrements de vidéosurveillance ou de vidéoprotection, par exemple, ne doivent pas, en principe, être conservés au-delà d'un mois. Les données à caractère personnel ayant trait à des clients, quant à elles, ne doivent pas être conservées au-delà d'un an à l'issue de la relation contractuelle au sein des dossiers courants. Toutefois, cette obligation de fixer une durée de conservation limitée dans le temps ne prive pas les responsables de traitements de la possibilité d'archiver des informations, notamment à des fins probatoires. Lorsque cet archivage est réalisé sous forme électronique, il convient de respecter la recommandation n° 2005-213 de la CNIL du 11 octobre 2005 relative à l'archivage électronique de données à caractère personnel dans le secteur privé.

3.1.4. Les principes de sécurité et de confidentialité

Les données contenues dans les fichiers ne peuvent être consultées que par les personnes habilitées à y accéder en raison de leurs missions. Les dossiers des avocats ne peuvent être communiqués qu'à des personnes autorisées à en connaître, notamment en application de dispositions législatives particulières et sous réserve du respect du secret professionnel.

L'avocat, en qualité de responsable du traitement, est astreint à une obligation de sécurité. Il doit ainsi prendre toutes les mesures nécessaires pour en garantir la confidentialité et éviter toute divulgation d'information.

Il convient, par exemple, de veiller à ce que chaque personne habilitée à accéder aux informations dispose d'un mot de passe individuel (composé, si l'authentification repose uniquement sur un identifiant et un mot de passe, de 12 caractères minimum et de majuscules, minuscules, chiffres et caractères spéciaux et renouvelé régulièrement) et que les droits d'accès soient précisément définis en fonction des besoins réels.

3.1.5. Le principe du respect des droits des personnes

L'article 13 du RGPD exige que soient communiquées les informations suivantes lorsque les données sont collectées auprès de la personne concernée :

- les coordonnées du responsable du traitement et, le cas échéant, celles du représentant du responsable du traitement ;
- le cas échéant, les coordonnées du délégué à la protection des données ;
- les finalités du traitement auquel sont destinées les données à caractère personnel ;
- la base juridique du traitement ;
- les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers lorsque ces intérêts légitimes sont la condition de licéité du traitement ;
- le fait que le responsable de traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ;
- le cas échéant, l'existence ou l'absence d'une décision d'adéquation rendue par la CNIL, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;
- la durée de conservation des données à caractère personnel ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

- l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données ;
- lorsque le traitement est fondé sur le consentement de la personne concernée, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;
- l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

L'article 14 du RGPD énumère quant à lui les informations à communiquer lorsque les données à caractère personnel ne sont pas directement collectées auprès de la personne concernée. C'est le cas notamment lorsque dans le cadre d'un dossier, le client transmet des informations sur la partie adverse à l'avocat. Ces informations contiennent des données à caractère personnel de la partie adverse qui seront dès lors indirectement collectées par l'avocat.

L'article 14 du RGPD prévoit donc que la personne doit être informée des éléments prévus à l'article 13 du RGPD mais également les catégories de données à caractère personnel concernées et la source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public.

Une telle information poserait difficulté à l'avocat puisque le respect de cette obligation impliquerait d'informer la partie adverse de la constitution du dossier par l'avocat et donc de mettre en péril les intérêts de son client. C'est pourquoi, le RGPD prévoit à l'article 14 alinéa 5, d) une exception à l'information des personnes dont les données à caractère personnel sont indirectement collectées, dès lors que lesdites données doivent rester confidentielles en vertu d'une obligation de secret professionnel réglementée.

Les avocats, lorsqu'ils agissent en qualité de responsable de traitement, sont libres de déterminer les moyens à mettre en œuvre pour assurer l'information des personnes.

Toute personne a le droit de s'opposer, pour un motif légitime, à ce que des données la concernant soient traitées, sauf si le traitement concerné présente un caractère obligatoire.

Par ailleurs, toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel notamment pour :

- savoir si des données qui la concernent y figurent ou non ;
- obtenir la communication des données qui la concernent sous une forme compréhensible, d'une part, et de toutes les informations disponibles quant à leurs origines, d'autre part ;
- obtenir des informations sur la finalité du traitement, les données collectées et les destinataires.

3.2. Nouvelles mesures de conformité

Le RGPD a pour objectif de moderniser le cadre européen de la protection des données à caractère personnel afin de prendre en compte les avancées technologiques et d'harmoniser les législations des États membres de l'Union européenne.

En pratique, il vise à :

- Renforcer les droits des personnes, notamment par la création de droits à la limitation, à l'oubli, à la portabilité des données à caractère personnel et par la création de dispositions propres aux personnes mineures ;
- Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
- Favoriser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des sanctions renforcées et des décisions communes concernant des traitements transnationaux.

Avec le RGPD, la responsabilité des organismes se trouve renforcée : ceux-ci devront à tout moment assurer une protection optimale des données et être en mesure de démontrer la conformité de leur traitement, ce qui implique de documenter cette conformité.

Les principales mesures imposées par le RGPD sont les suivantes :

- 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 ;
- Se conformer au principe d'accountability qui impose aux cabinets de se pré-constituer la preuve de leur conformité ;
- Notifier à la CNIL toute violation de données à caractère personnel ;
- Désigner, lorsque les conditions sont remplies, un Délégué à la protection des données ou Data Protection Officer (DPO).

L'avocat, lorsqu'il agit en qualité de responsable du traitement, a l'obligation, aux termes de l'article 28 du RGPD, de s'assurer que son prestataire informatique, en qualité de sous-traitant, a mis en place des mesures techniques et organisationnelles adaptées lui permettant de respecter la sécurité et la confidentialité des données. La conclusion d'un contrat est obligatoire entre l'avocat et ses sous-traitants et doit réserver une faculté d'audit pour permettre de vérifier la mise en œuvre conforme des mesures précitées.

3.2.1. Notification de toute violation de données à caractère personnel

En vertu des articles 33 et 34 du RGPD, un cabinet d'avocats agissant en tant que responsable de traitement doit notifier toute violation de données à caractère personnel à l'autorité de contrôle et communiquer auprès des personnes concernées en cas de risque élevé pour les droits et libertés des personnes.
A cet égard, il est renvoyé à la fiche pratique n°9 « Procédure en cas de violation de données ».

3.2.2. Minimisation des données

Le principe de minimisation des données, ou « limitation des données au minimum » est le principe selon lequel des données à caractère personnel ne peuvent faire l'objet d'un traitement que si, et pour autant que, les finalités du traitement ne peuvent être atteintes par le traitement d'informations ne contenant pas de données à caractère personnel.

Il consiste à :

- s'interroger sur la nécessité de traiter des données à caractère personnel pour atteindre les finalités recherchées par le traitement ;
- si le traitement de données à caractère personnel s'avère nécessaire, limiter le traitement des données au minimum, en ce qui concerne :
  - les catégories de données traitées ;
  - le volume ou la quantité de données traitées ;
  - la question de savoir si les données collectées sont plus ou moins nécessaires au traitement.

3.2.3. Droit à l'oubli

L'article 17 du RGPD prévoit le droit à l'effacement (« droit à l'oubli ») : les personnes concernées ont le droit d'obtenir du responsable du traitement, dans les meilleurs délais, l'effacement des données à caractère personnel les concernant.

Cette disposition trouve sa source dans l'affaire Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, dans laquelle la Cour a jugé que les personnes physiques sont en droit (sous réserve de certaines conditions et garanties) de demander à un moteur de recherche de supprimer les liens renvoyant à des données à caractère personnel les concernant. Le droit à l'oubli ou droit à l'effacement, inscrit dans le RGPD va bien au-delà du déréférencement visé dans l'arrêt Google précité. Il est cependant relatif et suppose que soit effectué un contrôle de proportionnalité entre les intérêts de la personne concernée et ceux du responsable du traitement, ou, le cas échéant du public en général (droit à l'information ou intérêt historique).

Pour l'avocat, l'effacement irréversible des données d'un client ne pourra être mis en œuvre avant l'expiration de la durée de prescription de la responsabilité civile professionnelle de l'avocat. Il est en effet important de noter que le droit à l'oubli ne prévaut évidemment pas sur certaines obligations d'archivage de données pendant des périodes déterminées, par exemple pour des raisons de conformité aux obligations fiscales ou de prescription.

3.2.4. Analyses d'impact

En vertu de l'article 35 du RGPD, lorsqu'un type de traitement est susceptible d'engendrer un **risque élevé pour les droits et libertés des personnes physiques**, notamment le **traitement à grande échelle de catégories particulières de données**, le responsable du traitement doit effectuer, avant toute mise en œuvre, une analyse d'impact.

Il est important de noter que le **considérant 91 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.**

Néanmoins, quand bien même il ne traiterait pas des données à « grande échelle », un cabinet d'avocats, quelque soit sa taille, pourrait avoir à réaliser des analyses d'impact si les traitements mis en œuvre répondent à certaines caractéristiques.

En effet, dès lors qu'il répondra à plus de deux des neuf critères déterminés par la CNIL et par le G29 (évaluation/scoring, décision automatique avec effet légal ou similaire ; surveillance systématique ; collecte de données sensibles ; collecte de données à caractère personnel à large échelle ; croisement de données ; personnes vulnérables ; usage innovant ; exclusion du bénéfice d'un droit / contrat), le traitement sera, par principe, soumis à analyse d'impact.

Bien qu'elles représentent une charge supplémentaire, les analyses d'impact visent à permettre aux responsables de traitements d'identifier et de traiter les risques qui n'auraient pas été détectés en d'autres temps et d'empêcher des violations qui se seraient autrement produites.

Pour expliquer l'article 35 et en proposer une interprétation commune, les autorités de protection des données européennes (le G29) ont adopté des « lignes directrices » sur les DPIA et les traitements susceptibles d'engendrer des risques :
https://www.cnil.fr/fr/reglement-europeen/lignes-directrices

Le 29 janvier 2018, la CNIL a mis en ligne sur son site la nouvelle version de son logiciel open source PIA facilitant la conduite et la formalisation d'analyses d'impact sur la protection des données telles prévues par le RGPD :
https://www.cnil.fr/fr/outil-pia-nouvelle-version-beta-du-logiciel.

La CNIL a également publié trois catalogues de bonnes pratiques destinées à traiter les risques que les traitements de données à caractère personnel (DCP) peuvent faire peser sur les libertés et la vie privée des personnes concernées :
https://www.cnil.fr/fr/PIA-privacy-impact-assessment

3.2.5. Portabilité des données

Définition. Le droit à la portabilité des données permet aux personnes concernées d'exiger des responsables de traitement la transmission de leurs données à caractère personnel à un autre responsable de traitement, sans que le responsable de traitement ayant initialement collecté les données puisse s'y opposer.

La portabilité emporte :

- « le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable de traitement, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable de traitement [...] ; »
- le droit d'obtenir que les données soient transmises directement d'un responsable de traitement à un autre lorsque « cela est techniquement possible[1] ».

Conditions. Cela signifie donc que l'avocat qui a initialement traité les données à caractère personnel est tenu de communiquer les données à caractère personnel relatives à son client ou à un confrère, lorsque le traitement initial repose sur l'un des fondements suivants :

- le client a exprimé son consentement au traitement de ses données à caractère personnel ou le traitement est nécessaire à l'exécution d'un contrat auquel le client est partie ou à l'exécution de mesures précontractuelles prises à la demande du client ;
- et le traitement est effectué à l'aide de procédés automatisés.

L'avocat devra donc faire droit à la demande de son client si celui-ci demande la transmission de ses données à caractère personnel à un confrère et les transmettre dans un format structuré, couramment utilisé et lisible par machine.

En revanche, le droit à la portabilité des données ne s'exerce pas lorsque 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[2].

L'exception des dossiers papiers. Selon le G29[3] « le droit à la portabilité des données s'applique uniquement si le traitement des données « est effectué à l'aide de procédés automatisés » et, par conséquent, ne couvre pas la plupart des dossiers papier ». Les dossiers papiers des avocats sembleraient donc exclus du droit à la portabilité des données personnelles.

Succession d'avocats dans un même dossier. En tout état de cause, les avocats sont soumis à des règles spécifiques s'agissant de la succession d'avocats dans un même dossier. En effet, l'article 9.2 du Règlement intérieur national de la profession d'avocat prévoit que « l'avocat dessaisi, ne disposant d'aucun droit de rétention, doit transmettre sans délai tous les éléments nécessaires à l'entière connaissance du dossier ».

1. Règl. (UE) n°2016-679 du 27-4-2016 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, article 20§2.
2. Règl. (UE) n°2016-679 du 27-4-2016 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, article 20§3.
3. Lignes directrices WP 242 du G29, p 11.

3.2.6. Capacité à suivre les destinataires de données à caractère personnel

Les responsables du traitement de données doivent être en mesure de suivre et d'identifier les destinataires des données à caractère personnel qu'ils traitent.

3.2.7. Tenue d'un registre des activités de traitement

Le RGPD impose, dans certains cas, aux responsables de traitement de tenir un registre des activités de traitement effectuées sous leur responsabilité.

A cet égard, il est renvoyé à la fiche pratique n°10 « Le registre des activités de traitement ».

FICHES PRATIQUES

FICHE N°1. LE TRAITEMENT « RH » (RESSOURCES HUMAINES)

1. Qu'est-ce qu'un traitement RH ?

Dans le cadre du recrutement d'un collaborateur ou encore du personnel support (par exemple un informaticien ou une secrétaire), de la gestion de la paie et de la gestion administrative du personnel, l'avocat employeur est amené à effectuer des traitements de données à caractère personnel.

Ainsi, les avocats doivent nécessairement effectuer ces traitements de données conformément au RGPD.

A cet égard, il convient de noter que l'article 88 du RGPD qui concerne le traitement de données à caractère personnel dans le cadre des relations au travail, dispose que les Etats membres conservent une marge de manœuvre quant aux règles à édicter.

2. Quelles sont les données que l'avocat peut collecter dans le cadre d'un traitement RH ?

Recrutement. Dans le cadre du recrutement, les données ne doivent servir qu'à évaluer la capacité du candidat à occuper l'emploi proposé.

Seules des données relatives à la qualification et à l'expérience du collaborateur peuvent être collectées (exemples : diplômes, emplois précédents, etc.)

Il est donc interdit de :

- Demander à un candidat son numéro de sécurité sociale ;
- Collecter des données sur la famille du candidat ;
- Collecter des données sur les opinions politiques ou l'appartenance syndicale du candidat.

Gestion administrative du personnel. Dans le cadre de la gestion de ses collaborateurs et de manière plus générale, de son personnel, l'avocat employeur peut collecter principalement deux types de données :

- Des données nécessaires au respect d'une obligation légale.
- Des données utiles à la (i) gestion administrative du personnel, (ii) à l'organisation du travail et (iii) à l'action sociale.

Respecter la minimisation. Dans le cadre des traitements RH et conformément à l'article 5 du RGPD, l'avocat ne doit collecter que des données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

Contrôle de l'activité du personnel. L'avocat employeur peut mettre en place différents outils afin de contrôler l'activité des collaborateurs ou du personnel.

Par exemple, le cabinet d'avocats pourrait encadrer les conditions d'utilisation d'Internet par les collaborateurs et le personnel sur leur lieu de travail. Il peut mettre en place des filtres afin de bloquer certains contenues (pornographie, pédophilie, etc.). Il est également possible de limiter l'utilisation d'Internet pour des raisons de sécurité par exemple le téléchargement de logiciels, la connexion à un forum, etc.

Contrôle du temps passé. Un cabinet peut mettre en place un logiciel permettant de calculer le temps passé par l'avocat sur un dossier ou une affaire. Cependant, ce logiciel ne peut être détourné afin de contrôler l'activité des collaborateurs.

Gestion et contrôle de l'accès au cabinet d'avocats. Un cabinet d'avocats peut mettre en place des dispositifs afin de contrôler les horaires et l'accès des collaborateurs et du personnel.

3. L'avocat doit-il procéder à des formalités en cas de traitement RH ?

Avant le 25 mai 2018. En application de la loi Informatique et libertés du 6 janvier 1978, les responsables de traitement devaient effectuer des déclarations auprès de la CNIL préalablement à la mise en œuvre d'un traitement de données à caractère personnel.

En matière de ressources humaines, la CNIL avait édicté des normes et autorisations pour simplifier ce processus, notamment la norme simplifiée n°46 qui concerne la gestion des ressources humaines des organismes publics et privés ainsi que la dispense DI-002 relative à la paie des personnels du secteur privé. Ces normes peuvent servir aux cabinets d'avocats pour les aider à déterminer les limites aux traitements des données personnelles.

Après le 25 mai 2018. Le RGPD allège grandement les formalités mais introduit en contrepartie de nouvelles obligations pour le responsable de traitement.

Le registre des activités de traitement. Le registre des activités de traitement répertorie les informations relatives aux caractéristiques des traitements mis en œuvre par le responsable de traitements.

Cette obligation ne s'impose que dans certains cas. A priori, le cabinet d'avocats doit tenir un registre des activités de traitements dans la mesure où il traite de manière non occasionnelle des données à caractère personnel et en particulier

des données sensibles (ex : données de santé, données sur l'origine raciale, etc.) ou des données se rapportant à des condamnations et des infractions pénales.

Il convient donc d'insérer dans le registre des activités de traitement, une fiche dédiée à la gestion des ressources humaines qui doit comporter les éléments suivants :

- Identité et coordonnées du responsable de traitement ;
- Finalités ;
- Catégories de personnes concernées ;
- Catégories de données à caractère personnel ;
- Catégories de destinataires ;
- Transferts vers un pays tiers ou une organisation internationale ;
- Délais prévus pour l'effacement ;
- Description générale des mesures de sécurité techniques et organisationnelles.

4. Combien de temps les données peuvent-elles être conservées ?

L'avocat responsable de traitement doit définir une politique de durée de conservation des données au sein de son cabinet. Les données à caractère personnel ne peuvent être conservées que le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte. Généralement, les données relatives aux collaborateurs ou au personnel sont conservées le temps de leur présence dans le cabinet d'avocats augmenté des durées de prescriptions légales.

5. Doit-il y avoir une information des personnes concernées ?

- Conformément aux exigences de l'article 13 du RGPD, les collaborateurs et le personnel du cabinet d'avocats doivent être informés :
- De l'identité et des coordonnées du responsable de traitement ;
- Des coordonnées du délégué à la protection des données lorsqu'il y en a un ;
- De l'objectif poursuivi (gestion administrative du personnel et du recrutement) ;
- De la base juridique du traitement ;
- De l'intérêt légitime s'il s'agit de la base légale du traitement ;
- Des destinataires des données (des sous-traitants de la gestion de paie, etc.) ;
- Des flux transfrontières ;
- De la durée de conservation ;
- Des conditions d'exercice de leurs droits d'opposition, d'accès, de rectification et de limitation, etc. ;
- Du droit de retirer son consentement s'il s'agit de la base légale du traitement ;
- Du droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- Des informations sur le caractère réglementaire ou contractuel du traitement lorsqu'il s'agit de la base légale du traitement.

Ces informations peuvent figurer sur le contrat de collaboration ou sur le contrat de travail. Ces informations peuvent également faire l'objet d'un affichage ou d'une communication par courriel, notamment pour régulariser la situation auprès des collaborateurs et du personnel qui n'ont pas été correctement informés.

À FAIRE	
Vérifier que les données collectées ne sont pas excessives au regard de la finalité du traitement	☐
Vérifier qu'il y a une base légale au traitement de données personnelles	☐
Respecter le principe de minimisation	☐
Vérifier les dispositifs de contrôle de l'activité du personnel et leur pertinence	☐
Avant le 25 mai 2018 : procéder aux formalités nécessaires	☐
Après le 25 mai 2018 : procéder à la tenue du registre des traitements	☐
Définir une politique de durée de conservation	☐
Informer les personnes concernées sur le traitement de leurs données personnelles	☐

FICHE N°2. GESTION DES CLIENTS

1. Quelles données l'avocat peut-il collecter dans le cadre de la gestion de ses clients ?

Dans le cadre de l'exercice de la profession d'avocat, les données à caractère personnel relatives à la gestion de la clientèle correspondent à toutes les données à caractère personnel nécessaires dans la constitution du dossier du client et dans la défense de ses intérêts.

Au regard de la diversité des domaines d'intervention des avocats, ces données peuvent être très diverses et peuvent concerner des données relatives tant à la vie personnelle qu'à la vie professionnelle mais peuvent concerner également des données d'une particulière sensibilité.

Données relatives aux condamnations pénales et aux infractions. L'avocat peut être amené à collecter des données relatives aux condamnations pénales et aux infractions. Le caractère particulier de ces données appelle à des garanties spécifiques de traitement. Ainsi, l'article 10 du RGPD prévoit qu'un tel traitement ne peut être effectué que sous le contrôle de l'autorité publique, ou si des garanties spécifiques et adaptées sont prévues par le droit national[4].

Toutefois, la loi Informatique et libertés[5] prévoit que le traitement de telles données peut être effectué par les **auxiliaires de justice pour exercer les missions que la loi leur confie.**

Le projet de loi relatif à la protection des données personnelles, en l'état actuel de sa rédaction, maintient cette exception permettant aux auxiliaires de justice de traiter des données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes.

Catégories particulières de données. L'avocat peut être amené à traiter des données personnelles dites particulières qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Or, l'article 9, al.1, du RGPD prévoit l'interdiction de principe du traitement de telles données. Ce traitement de données particulières peut concerner un grand nombre d'avocats, notamment ceux spécialisés en droit de la santé ou encore en droit du dommage corporel.

4. Règl. (UE) 2016/679 du 27-4-2016, art. 10 et considérant 19
5. Loi n° 78-17 du 6-1-1978 modifiée, art. 9.

Cependant, l'article 9 prévoit une exception à l'alinéa 2.f) pour « le traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ». Il semble donc que les avocats jouissent d'une exception leur permettant de traiter de données particulières afin d'exercer leur profession pour autant que la donnée concernée soit strictement nécessaire à la constatation, à l'exercice ou à la défense du droit de son client en justice. Une appréciation stricte de cette nécessité est bien entendu recommandée.

Respect du principe de minimisation. Conformément à l'article 5 du RGPD, l'avocat ne doit collecter que des données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

Or, il n'est pas rare que l'avocat reçoive beaucoup d'informations de ses clients. Afin de respecter le principe de minimisation, il convient, autant que faire se peut, d'orienter son client lorsqu'il fournit des données personnelles à l'avocat sur les documents qui sont nécessaires pour le représenter et le conseiller.

2. L'avocat doit-il procéder à des formalités ?

Avant le 25 mai 2018. En application de la loi Informatique et libertés du 6 janvier 1978, les responsables de traitement devaient effectuer des déclarations auprès de la CNIL préalablement à la mise en œuvre d'un traitement de données à caractère personnel.

En matière de gestion des clients, la CNIL avait édicté des dispenses et normes pour simplifier ce processus, notamment la norme simplifiée n°48 qui concerne la gestion des fichiers clients et prospects ainsi que la dispense DI-007 relative à l'information et la communication externe. Ces normes peuvent servir aux cabinets d'avocats pour les aider à déterminer les limites aux traitements des données personnelles.

Après le 25 mai 2018. Le RGPD allège grandement les formalités mais introduit en contrepartie de nouvelles obligations pour le responsable de traitement.

Le registre des activités de traitement. Le registre des activités de traitement répertorie les informations relatives aux caractéristiques des traitements mis en œuvre par le responsable de traitements.

Cette obligation ne s'impose que dans certains cas. A priori, le cabinet d'avocats doit tenir un registre des activités de traitements dans la mesure où il traite de manière non occasionnelle des données à caractère personnel et en particulier des données sensibles (ex : données de santé, données sur l'origine raciale, etc.) ou des données se rapportant à des condamnations et des infractions pénales.

Il convient donc d'insérer dans le registre des activités de traitement, une fiche dédiée à la gestion des clients qui doit comporter les éléments suivants :

- Identité et coordonnées du responsable de traitement
- Finalités ;

- Catégories de personnes concernées ;
- Catégories de données à caractère personnel ;
- Catégories de destinataires ;
- Transferts vers un pays tiers ou une organisation internationale ;
- Délais prévus pour l'effacement ;
- Description générale des mesures de sécurité techniques et organisationnelles.

3. Combien de temps les données peuvent-elles être conservées ?

L'avocat responsable de traitement doit définir une politique de durée de conservation des données au sein de son cabinet. Les données à caractère personnel ne peuvent être conservées que le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte.

Généralement, les données relatives aux clients peuvent être conservées le temps de la relation contractuelle entre l'avocat et son client. Au-delà, les données devraient être archivées pour la période où la responsabilité de l'avocat pourrait être mise en cause avant suppression définitive des données.

4. Doit-il y avoir une information des personnes concernées ?

Conformément aux exigences de l'article 13 du RGPD, les clients et prospects du cabinet d'avocats doivent être informés :

- De l'identité et des coordonnées du responsable de traitement (le cabinet) ;
- Des coordonnées du délégué à la protection des données lorsqu'il y en a un ;
- De l'objectif poursuivi (gestion et suivi des dossiers de ses clients) ;
- De la base juridique du traitement (exécution contractuelle ou précontractuelle à la demande du client) ;
- De l'intérêt légitime s'il s'agit de la base légale du traitement ;
- Des destinataires des données (des sous-traitants, des huissiers, etc.) ;
- Des flux transfrontières ;
- De la durée de conservation ;
- Des droits dont ils disposent ;
- Des conditions d'exercice de ces droits ;
- Du droit de retirer son consentement s'il s'agit de la base légale du traitement ;
- Du droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- Des informations sur le caractère réglementaire ou contractuel du traitement lorsqu'il s'agit de la base légale du traitement.

Ces informations peuvent figurer au sein de la convention d'honoraires. Ces informations peuvent également faire l'objet d'une communication par courriel ou à l'occasion de la transmission d'une note d'honoraires, notamment pour régulariser la situation auprès des clients qui n'ont pas été correctement informés.

5. La sécurité des dossiers clients

Il est nécessaire de prendre des mesures de sécurité adaptées à la sensibilité des traitements. Au-delà de cette exigence du RGPD, l'avocat est soumis au secret professionnel absolu et se doit, encore plus pour cette raison, d'assurer la sécurité des données qui lui sont confiées par ses clients.

Pour ce faire, il est nécessaire de vérifier que l'accès aux locaux dans lesquels sont stockés les dossiers est suffisamment sécurisé (bureaux fermés à clefs, accès par badge, etc.). Il convient également de vérifier la sécurité du système d'information sur lequel sont stockés les dossiers sous format numérique (pare-feu, mots de passe robustes pour y accéder, habilitations, etc.).

6. Sollicitation personnalisée

Au-delà du respect des exigences précitées, des règles particulières s'appliquent en matière de sollicitation personnalisée par voie électronique ou par voie postale.

A cet égard, il est renvoyé au Vademecum de la communication des avocats publié en 2016 par le Conseil national des barreaux :

http://encyclopedie.avocats.fr/GED_BWZ/107763592594/CNB-2016-03-17_Ru_Communication-des-avocats-Vade-mecum[Version-2016-03-16].pdf

À FAIRE	
Vérifier que les données collectées ne sont pas excessives au regard de la finalité du traitement	☐
Vérifier qu'il y a une base légale au traitement de données personnelles	☐
Respecter le principe de minimisation	☐
Avant le 25 mai 2018 : procéder aux formalités nécessaires	☐
Après le 25 mai 2018 : procéder à la tenue du registre des traitements	☐
Définir une politique de durée de conservation	☐
Informer les personnes concernées sur le traitement de leurs données personnelles	☐
Vérifier que les dossiers clients numériques et physiques sont correctement protégés	☐
Vérifier la sécurité du système d'information auprès de son prestataire informatique	☐

FICHE N°3. VIDÉOSURVEILLANCE ET VIDEOPROTECTION

1. Qu'est-ce que la vidéosurveillance et la vidéoprotection ?

Selon le lieu où les caméras sont installées, le régime applicable diffère. En effet, il est nécessaire de distinguer la vidéoprotection de la vidéosurveillance puisque chacune a son propre régime :

- La **vidéoprotection** vise les caméras situées dans les locaux ouverts au public, à savoir par exemple les SAS d'entrée, les abords directs d'un immeuble et de l'accueil d'un immeuble où serait situé le cabinet d'avocats.
- La **vidéosurveillance** vise les caméras installées dans les zones réservées aux membres du cabinet comme par exemple les bureaux, les réserves ou les couloirs du cabinet d'avocats, etc.

Quel que soit le régime applicable, la CNIL est compétente pour opérer des contrôles sur les dispositifs de vidéoprotection comme sur les dispositifs de vidéosurveillance.

2. Quel est l'objectif de l'installation de caméras ?

L'installation de caméras de vidéoprotection et de vidéosurveillance doit avoir pour finalité la sécurité des biens et des personnes lorsque ces lieux sont particulièrement exposés à des risques d'agression ou de vol, à titre dissuasif ou pour permettre l'identification des auteurs de vols, de dégradations ou d'agressions.

En vertu du droit au respect de la vie privée (article 9 du Code civil), la vidéosurveillance ne peut en aucun cas servir à filmer les membres du cabinet sur leur poste de travail, dans les zones de pause ou de repos, dans les toilettes ou encore dans les locaux syndicaux ou des représentants du personnel.

3. Quelles sont les formalités à accomplir ?

3.1. Avant l'entrée en vigueur du RGPD

Les dispositifs de vidéoprotection et de vidéosurveillance sont très encadrés et ne peuvent être mis en œuvre qu'après l'accomplissement de certaines formalités.

Les formalités sont différentes selon le type de dispositif mis en place.

Si les caméras sont soumises aux dispositions du Code de la sécurité intérieure, alors une autorisation de la préfecture du département (Préfet de police à Paris) est nécessaire (art. L251-1 et suivants du Code de la sécurité intérieure).

Si les caméras sont soumises aux dispositions de la loi Informatique et libertés, alors elles doivent faire l'objet d'une déclaration normale auprès de la CNIL.

TYPE DE DISPOSITIF	EXEMPLE	FORMALITÉS À ACCOMPLIR
La caméra est située dans le cabinet d'avocats fermé au public	Bureaux, réserves, salle de reprographie, couloirs du cabinet d'avocats, etc.	Formalités préalables auprès de la CNIL
La caméra est située dans un lieu public ou ouvert au public et **les images sont enregistrées ou conservées** dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques	Salle d'attente, immeuble du cabinet d'avocats, hall d'entrée, etc.	Autorisation préfectorale
La caméra est située dans un lieu public ou ouvert au public et **aucune image n'est enregistrée ni conservée** dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques		

3.2. Après l'entrée en vigueur du RGPD

Le RGPD introduit de nouvelles obligations pour le responsable de traitement.

Le registre des activités de traitement. Le registre des activités de traitement répertorie les informations relatives aux traitements mis en œuvre.

Cette obligation ne s'impose que dans certains cas. A priori, le cabinet d'avocats doit tenir un registre des activités de traitements dans la mesure où il traite de manière non occasionnelle des données à caractère personnel et en particulier des données sensibles (ex : données de santé, données sur l'origine raciale, etc.) ou des données se rapportant à des condamnations et des infractions pénales.

Il convient donc d'insérer dans le registre des activités de traitement une fiche dédiée à la vidéo surveillance/ la vidéoprotection qui doit comporter les éléments suivants :

- Identité et coordonnées du responsable de traitement ;
- Finalités ;
- Catégories de personnes concernées ;
- Catégories de données personnelles ;
- Catégories de destinataires ;
- Transferts vers un pays tiers ou une organisation internationale ;
- Délais prévus pour l'effacement des données ;
- Description générale des mesures de sécurité techniques et organisationnelles.

4. Est-il nécessaire d'informer les personnes concernées ?

Les personnes concernées, à savoir par exemple les clients, les membres du cabinet, les confrères ou encore les prestataires, doivent être informés de l'existence du dispositif mis en place.

Cette information doit être assurée au moyen d'un panneau affiché de façon visible dans les lieux et locaux concernés (entrée de l'établissement). Cette information doit porter a minima sur :

- l'existence du dispositif ;
- le nom de son responsable ;
- la procédure à suivre pour demander l'accès aux enregistrements visuels les concernant ;
- le numéro de téléphone.

Les instances représentatives du personnel, si elles existent au sein du cabinet, devront être consultées avant la mise en œuvre du système de vidéosurveillance.

En tout état de cause, chaque membre du cabinet devra être informé individuellement, au moyen d'une note de service qui peut prendre la forme d'un courriel par exemple, et qui est conforme aux exigences des articles 13 et 14 du RGPD.

5. Qui peut accéder aux images des caméras ?

Les images enregistrées par les caméras de vidéoprotection et de vidéosurveillance ne peuvent être visionnées que par les seules personnes habilitées dans le cadre de leurs fonctions (associé fondateur ou la personne responsable de la sécurité par exemple). Ces personnes doivent être particulièrement formées et sensibilisées aux règles encadrant la mise en place d'un tel système.

6. Combien de temps les images peuvent-elles être conservées ?

S'agissant de la durée de conservation, la CNIL indique que les images ne devraient pas être conservées plus de quelques jours et qu'en tout état de cause, leur durée de conservation ne peut pas excéder un mois.

Si des procédures sont engagées, les images doivent alors être extraites du dispositif (après consignation de cette opération dans un cahier spécifique) et conservées pour la durée de la procédure.

THÈME	À FAIRE	
GÉNÉRAL	Identifier les caméras	☐
	Déterminer la localisation des caméras et les lieux filmés	☐
	Limiter l'accès aux images enregistrées	☐
	Après le 25 mai 2018 : mettre en place un registre des activités de traitements (recommandé)	☐
	Afficher un panneau visible dans les lieux et locaux concernés	☐
	Consulter les instances représentatives du personnel avant l'installation des caméras	☐
	Informer individuellement le personnel (notamment par courriel)	☐
	Limiter la durée de conservation des images à un mois	☐
VIDÉOPROTECTION	Procéder à une demande d'autorisation auprès de la préfecture du département	☐
VIDÉOSURVEILLANCE	Avant le 25 mai 2018 : Déclaration normale auprès de la CNIL en présence de traitement de données personnelles	☐

Pour en savoir plus :

https://www.cnil.fr/sites/default/files/atoms/files/_videosurveillance_au_travail.pdf

FICHE N°4.
FOURNISSEURS ET PRESTATAIRES

1. Qu'est-ce qu'un sous-traitant ?

En vertu de l'article 4, al. 8, du RGPD, le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement ».

En pratique, il s'agit donc de la personne qui traite des données à caractère personnel pour le compte du cabinet d'avocats comme par exemple un comptable, un éditeur de logiciel, un hébergeur, etc.

2. Que faire en cas de sous-traitance ?

L'article 28, al. 3, du RGPD maintient l'obligation de souscrire un contrat liant le sous-traitant au responsable du traitement, tout en précisant ses contours et en fixant des exigences strictes et plus importantes. Ainsi, le contrat liant le cabinet au sous-traitant doit comporter :

- l'objet ;
- la durée ;
- la nature ;
- la finalité ;
- le type de données à caractère personnel ;
- les catégories de personnes concernées ;
- les droits et obligations du responsable de traitement ;
- les mesures de sécurité mises en œuvre concernant le traitement de données à caractère personnel qui sera réalisé.

L'acte juridique en question doit également définir les obligations du sous-traitant relatives à :

- la possibilité de ne traiter les données que sur instruction documentée du responsable du traitement, même en ce qui concerne les flux transfrontières ;
- la confidentialité des données ;
- l'exercice des droits des personnes concernées ;
- l'aide qu'il doit fournir au responsable de traitement par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, pour s'acquitter de l'obligation de donner suite aux demandes des personnes concernées ;

- l'aide fournie au responsable de traitement pour garantir le respect de ses obligations compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;
- la suppression des données concernées à l'issue du traitement, ou leur renvoi au responsable de traitement ou leur conservation s'il en est tenu par une disposition nationale ou européenne ;
- la mise à disposition du responsable du traitement de toutes les informations nécessaires pour démontrer le respect de ces obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;
- l'éventuel recrutement par le sous-traitant d'un sous-traitant ultérieur, d'un nouveau sous-traitant, et l'obtention de l'autorisation préalable écrite du responsable de traitement relative à ce recrutement qui doit être formalisé par un contrat mentionnant l'ensemble des obligations ci-dessus énumérées.

Les clauses contractuelles liant sous-traitants et responsables de traitement vont donc devoir être beaucoup plus précises tant sur les modalités de traitement que sur la gestion de leurs relations et l'échange d'informations entre eux.

En vertu de l'article 28, al.1, du RGPD, le responsable de traitement a l'obligation de ne recourir qu'à « des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée ».

3. Que faire avec les sous-traitants avec lesquels le cabinet est déjà en relation commerciale ?

Les cabinets d'avocats devront interroger leurs sous-traitants sur les garanties qu'ils ont mises en place afin de garantir leur conformité au RGPD.

Dans le cas où le cabinet d'avocats identifie des lacunes dans les mesures mises en place par le sous-traitant, ils devront conclure un avenant au contrat afin de combler lesdites lacunes.

À FAIRE	
Identifier les différents sous-traitants	☐
Vérifier la conformité des sous-traitants et les mesures mises en place dans le contrat de sous-traitance	☐
Conclure un avenant au contrat de sous-traitance si nécessaire	☐

FICHE N°5. LA GESTION DES ACCES AU CABINET

Sur le lieu de travail, les associés agissant en qualité d'employeur peuvent être amenés à contrôler les accès aux locaux ou la gestion de la restauration (badges électroniques, dispositifs biométriques...). De la même manière, des contrôles d'accès peuvent être mis en place pour les visiteurs du cabinet d'avocats.

1. L'utilisation de badges sur le lieu de travail

Des badges électroniques (cartes magnétiques ou à puce) peuvent servir au contrôle des accès aux locaux ou à la gestion de la restauration. Ces dispositifs, qui traitent des données permettant l'identification des personnes concernées, sont soumis au RGPD et doivent offrir toutes les garanties offertes par celui-ci aux personnes faisant l'objet d'une collecte et d'un traitement de leurs données personnelles.

Quelles garanties prévoir ?

Chaque passage du badge dans un lecteur permet l'enregistrement de données relatives à son détenteur. Ces enregistrements présentent des risques d'utilisation détournée et sont susceptibles de tracer les déplacements des avocats et salariés à des fins de surveillance.

Des garanties particulières doivent donc être apportées par le cabinet pour éviter de tels détournements. Il convient notamment de préciser :

- la finalité du dispositif (ex : contrôle des accès, gestion des temps de présence des salariés, gestion de la restauration ...) ;
- les informations collectées ;
- les services destinataires des données ;
- les modalités d'exercice des droits d'accès aux données et de rectification des données.

Les membres d'un cabinet d'avocats doivent être parfaitement informés de ces modalités, préalablement à la mise en œuvre du système.

Les cabinets d'avocats peuvent se référer aux préconisations de la norme NS 42 de la CNIL pour ce type de traitement :

https://www.cnil.fr/fr/declaration/ns-042-badges-sur-le-lieu-de-travail

À FAIRE	
Informer les membres du cabinet des modalités	☐
Se référer aux préconisations de la norme NS 42 de la CNIL	☐

2. Les dispositifs biométriques

La gestion des accès peut se faire par l'intermédiaire de dispositifs biométriques qui permettent d'identifier une personne par ses caractéristiques physiques, biologiques, voire comportementales (séquence génétique, reconnaissance faciale, empreintes digitales, etc.).

L'article 9 du RGPD considère ce type de données comme particulièrement sensible.

Le traitement de ce type de données est par principe interdit, sauf exceptions : ces données ne peuvent être traitées que si des conditions spécifiques ont été remplies et doivent être traitées avec des précautions supplémentaires et des mesures de sécurité.

Les personnes concernées par un dispositif biométrique doivent être clairement informées de ses conditions d'utilisation, de son caractère obligatoire ou facultatif, des destinataires des informations et des modalités d'exercice de leurs droits d'opposition, d'accès et de rectification.

La CNIL a adopté deux autorisations uniques qui encadrent désormais l'ensemble des dispositifs de contrôle d'accès biométrique sur les lieux de travail, quels que soient les types de biométries utilisées.

Elles distinguent :

- Les dispositifs biométriques permettant aux personnes de garder la maîtrise de leur gabarit biométrique (AU-052).
- Les dispositifs biométriques ne garantissant pas cette maîtrise (AU-053).

Les autorisations uniques adoptées s'inscrivent dans la logique du RGPD. Elles intègrent les prérequis de l'analyse d'impact sur la vie privée et les concepts de protection des données dès la conception du produit et par défaut (« privacy by design » et « privacy by default »), auxquels les responsables de traitement devront se conformer d'ici mai 2018.

La CNIL entend accompagner dès à présent les organismes dans leur mise en conformité à ces nouvelles règles.

À FAIRE	
Informer les personnes concernées	☐
Se référer aux autorisations uniques adoptées par la CNIL	☐

FICHE N°6. LA LUTTE CONTRE LE BLANCHIMENT ET LE FINANCEMENT DU TERRORISME

La règlementation qui encadre la lutte contre le blanchiment et le financement du terrorisme, met à la charge des avocats un certain nombre d'obligations, dont certaines consistent en des opérations de collecte et de traitement de données à caractère personnel au sens du RGPD.

La collecte des données et leur traitement réalisé sur ce fondement, qui est imposé par la loi, obéit en grande partie à un régime particulier et spécifique.

L'avocat qui noue une « relation d'affaires » avec un client doit exercer une vigilance constante pendant toute sa durée et doit pratiquer « un examen attentif des opérations effectuées en veillant à ce qu'elles soient cohérentes avec la connaissance actualisée » qu'il a de la relation d'affaires (art. L. 561-6 et R. 561-12 CMF).

Il doit en outre recueillir « les informations relatives à l'objet et à la nature de cette relation et tout autre élément d'information pertinent sur ce client ».

Il actualise ces informations pendant toute la durée de la relation d'affaires (art. L. 561-5-1, al. 1er CMF).

Ainsi, concernant une personne physique, l'avocat doit se voir présenter l'original d'un document officiel en cours de validité comportant la photographie du client (art. R. 561-5, 1 et R. 561-6 CMF).

À FAIRE	
Photocopier ou scanner le document d'identité du client, en conserver la copie et vérifier autant que possible s'il s'agit d'un faux	☐
Relever et conserver dans un document spécifique les mentions suivantes : • nom • prénoms • date et lieu de naissance de la personne • nature, date et lieu de délivrance du document, • nom et qualité de l'autorité ou de la personne qui a délivré le document et, le cas échéant, l'a authentifié	☐

Le Conseil national des barreaux met à la disposition des avocats un formulaire-type pouvant être remis au client et permettant d'appuyer de manière objective la demande de documents et renseignements :

https://www.cnb.avocat.fr/sites/default/files/documents/cahier_blanchiment_2ed.pdf.

Les mesures de vigilance et d'identification doivent être renforcées lorsque l'opération paraît particulièrement complexe ou d'un montant inhabituellement élevé ou ne paraît pas avoir de justification économique ou d'objet licite (art. L. 561-10-2 CMF).

Il faut alors se renseigner et obtenir des éléments complémentaires en posant des questions complémentaires.

Si les informations obtenues ne sont pas jugées suffisantes, l'avocat doit consigner par écrit et conserver les caractéristiques de l'opération, c'est-à-dire les renseignements recueillis et documentés concernant en particulier :

- l'origine et la destination des sommes ayant servi à financer l'opération,
- l'objet de l'opération,
- les caractéristiques de l'opération au regard des quatre conditions cumulatives énoncées ci-dessus,
- l'identité du client donneur d'ordre et du ou des ayants droit économiques, en précisant pour chacun d'eux le nom, l'adresse, la nationalité et la profession.

Eu égard au pouvoir de contrôle dont dispose le conseil de l'Ordre en application de l'article 17, 13°, de la loi du 31 décembre 1971, l'avocat doit pouvoir justifier auprès du conseil de l'Ordre, le cas échéant, que l'étendue des mesures qu'il a prises est appropriée au degré de risque (art. L. 561-5 CMF, art. L.561-9, I CMF). La bonne observation des prescriptions règlementaires ci-dessus, étant déjà un élément de preuve des diligences accomplies et du respect de son devoir de vigilance.

Les documents et informations, quel qu'en soit le support, relatifs à l'identité des clients habituels ou occasionnels doivent être conservés pendant **cinq ans** à compter de la cessation des relations avec eux (art. L. 561-12 CMF).

Il en va de même, sous réserve des obligations liées à l'exercice professionnel de l'avocat, pour les documents relatifs aux opérations qu'il a effectuées et pour les documents consignant les caractéristiques des opérations pour son compte propre ou pour le compte de tiers effectuées avec des personnes physiques ou morales, y compris leurs filiales ou établissements, domiciliés, enregistrés ou établis dans un État ou un territoire dont la législation en matière de lutte contre le blanchiment est jugée insuffisante (art. L. 561-12 CMF).

Les traitements en question identifiant des personnes susceptibles de participer à des infractions graves étant en effet particulièrement sensibles, l'obligation de sécurité des données ainsi collectées, mise à la charge des responsables de traitement par le RGPD, doit ici s'exprimer pleinement.

FICHE N°7. SITES INTERNET

Les avocats peuvent créer des sites Internet dans le cadre de leur activité professionnelle afin de promouvoir leur cabinet, présenter les membres du cabinet, exposer leurs compétences ou publier des articles mais le site Internet peut aussi permettre de collecter des données à caractère personnel par divers moyens :

- un questionnaire en ligne ;
- une consultation en ligne ;
- un formulaire de contact ;
- la création d'un compte en ligne ;
- des cookies, etc

1. Quelles sont les formalités à accomplir si l'avocat collecte des données à caractère personnel via son site internet ?

Avant le 25 mai 2018, le fichier peut faire l'objet d'une déclaration auprès de la CNIL :

- Si le fichier est conforme à une norme simplifiée, alors il faut procéder à une déclaration de conformité à cette norme. Par exemple, la norme simplifiée n°48 pour les fichiers clients-prospects ;
- Si le fichier n'est conforme à aucune norme, il faut procéder à une déclaration normale.

Après le 25 mai 2018. Le RGPD allège grandement les formalités mais introduit, en contrepartie, de nouvelles obligations pour le responsable de traitement.

Le registre des activités de traitement. Le registre des activités de traitement répertorie les informations relatives aux caractéristiques des traitements mis en œuvre par le responsable de traitement.

Cette obligation ne s'impose que dans certains cas. A priori, le cabinet d'avocats doit tenir un registre des activités de traitements dans la mesure où il traite de manière non occasionnelle des données à caractère personnel et en particulier des données sensibles (ex : données de santé, données sur l'origine raciale, etc.) ou des données se rapportant à des condamnations et des infractions pénales.

Il convient donc d'insérer dans le registre des activités de traitement, une fiche dédiée aux traitements de données sur le site Internet qui doit comporter les éléments suivants :

- Identité et coordonnées du responsable de traitement ;
- Finalités ;
- Catégories de personnes ;
- Catégories de données à caractère personnel ;
- Catégories de destinataires ;
- Transferts vers un pays tiers ou une organisation internationale ;
- Délais prévus pour l'effacement ;
- Description générale des mesures de sécurité techniques et organisationnelles.

2. Quelles sont les mentions qui doivent être obligatoirement présentes sur le site Internet de l'avocat ?

Plusieurs informations doivent figurer sur le site Internet de l'avocat :

- Les mentions légales en vertu de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;
- Les mentions obligatoires en vertu des articles 10.2 et 10.3 du RIN (Fiche n°4 du vade-mecum de la communication des avocats : http://encyclopedie.avocats.fr/GED_BWZ/107763592594/CNB-2016-03-17_Ru_Communication-des-avocats-Vade-mecum[Version-2016-03-16].pdf) ;
- Les mentions d'informations issues des articles 13 et 14 du RGPD ;
- Les mentions d'informations relatives aux cookies.

3. Que doivent contenir les différentes mentions ?

MENTIONS	TEXTES	INFORMATIONS
MENTIONS LÉGALES	Article 6 de la Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique	Dénomination et raison sociale du cabinet
		Adresse du cabinet principal
		Numéro d'inscription au registre du commerce et des sociétés (quand cette inscription est requise)
		Coordonnées postales, téléphoniques et électroniques du cabinet
		Nom et coordonnées du directeur de publication du site
		Nom, raison sociale, adresse et numéro de téléphone de l'hébergeur du site

MENTIONS	TEXTES	INFORMATIONS
MENTIONS OBLIGATOIRES	**Article 10.2 « Dispositions communes à toute communication » du Règlement Intérieur National de la profession d'avocat - RIN.**	Précision de la qualité (avocat)
		Identification (Me X, Cabinet X)
		Fourniture des informations sur sa localisation (adresse professionnelle)
		Eléments permettant de le joindre (n° tél, n° fax, adresse courriel),
		Mention du barreau auprès duquel l'avocat est inscrit
		Précision de la structure d'exercice à laquelle il appartient
		Le cas échéant, précision du réseau dont l'avocat est membre
MENTIONS D'INFORMATION RGPD	**Articles 13 et 14 du RGPD** **Article 32 de la loi Informatique et libertés**	L'identité et les coordonnées du responsable du fichier
		Les coordonnées du délégué à la protection des données
		La finalité et la base juridique du traitement
		Les intérêts légitimes poursuivis s'il s'agit de la base légale du traitement
		Les destinataires ou les catégories de destinataires
		La durée de conservation des données
		Les éventuels transferts de données vers des pays hors UE
		Les droits des personnes concernées (droit d'accès, de rectification, d'effacement, d'opposition, de limitation, etc.)
		Le droit de retirer son consentement à tout moment s'il s'agit de la base légale du traitement
		Le droit d'introduire une réclamation auprès d'une autorité de contrôle
		Les informations sur le caractère réglementaire ou contractuel du traitement s'il s'agit de la base légale du traitement

MENTIONS	TEXTES	INFORMATIONS
MENTIONS D'INFORMATION RELATIVES AUX COOKIES	Les directives du 25 novembre 2011 dites « Paquet télécom » 2009/136/CE et 2009/140/CE Ordonnance « Paquet télécom » du 24 août 2011 Article 32 II de la loi du 6 janvier 1978 Le projet e-Privacy	Les finalités des cookies Le recueil du consentement des utilisateurs via « les bandeaux de consentement » Les possibilités de refus des cookies

4. Qu'est-ce qu'un cookie ?

Les cookies sont des traceurs déposés et lus lors de la consultation du site Internet du cabinet d'avocats, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel.

Les cookies et autres traceurs ont généralement pour finalité d'analyser la navigation et la fréquentation du site Internet du cabinet d'avocats.

5. Comment rendre conforme l'utilisation des cookies sur le site Internet de l'avocat ?

Dans un premier temps, il est conseillé aux avocats de vérifier la présence effective de cookies sur leur site Internet par le biais du service informatique du cabinet, des prestataires ou en vérifiant les outils utilisés, etc.

Ensuite, il convient de déterminer les types de cookies utilisés sur le site Internet de l'avocat. En effet, certains cookies nécessitent le consentement de l'utilisateur, c'est le cas pour :

- les cookies publicitaires ;
- les cookies « réseaux sociaux » générés par les boutons de partage lorsqu'ils collectent des données à caractère personnel sans consentement des personnes concernées ;
- certains cookies de mesure d'audience.

Dans ce cas, le consentement doit être préalable à l'insertion ou à la lecture de cookies. Tant que le client n'a pas donné son consentement, ces cookies ne peuvent être déposés ou lus sur son terminal.

À FAIRE	
Intégration des mentions légales et obligatoires	☐
Intégration des mentions RGPD	☐
Avant le 25 mai 2018 : Déclarations CNIL s'il y a des traitements de données à caractère personnel	☐
Après le 25 mai 2018 : Registre des activités de traitements	☐
Identification de la présence de cookies mis en place sur le site Internet de l'avocat	☐
Identification du type de cookies présents sur le site Internet	☐
Mise en place d'un bandeau de recueil du consentement	☐
Intégration de mentions sur les cookies	☐

FICHE N°8. BONNES PRATIQUES DE SECURITE DES DONNEES

1. Pourquoi la sécurité des données à caractère personnel est particulièrement importante dans les traitements opérés par l'avocat ?

Il est essentiel d'assurer la sécurité et la confidentialité des données traitées par les cabinets d'avocats en garantissant un niveau de sécurité adapté au risque du traitement.

En effet, l'avocat est soumis au secret professionnel. Cette obligation renforce la nécessité de mettre en place des mesures de sécurité dans les cabinets d'avocats puisqu'en cas de violations des données à caractère personnel des clients, c'est le secret professionnel qui est violé. L'enjeu de la sécurité n'est donc pas anodin pour l'avocat.

2. Quelles mesures de sécurité physiques dois-je mettre en place ?

Il est nécessaire de mettre en place des mesures de sécurité physique dans votre cabinet :

- Limiter l'accès au cabinet ;
- Ne pas stocker ou archiver des dossiers ou documents contenant des données à caractère personnel dans des bureaux accessibles à tous ;
- Installer des alarmes dans les locaux du cabinet, etc.

3. Quelles mesures de sécurité logiques/numériques dois-je mettre en place ?

La mise en œuvre des mesures de sécurité permet de garantir un niveau de sécurité adapté au risque.

Il est notamment conseillé de :

- **authentifier les utilisateurs :** mettre en place un mot de passe de minimum 8 caractères contenant une majuscule, une minuscule, un chiffre et un caractère spécial ; ne pas le partager ; ne pas le noter en clair sur une feuille ; éviter de le préenregistrer ; le changer régulièrement.

- **gérer les habilitations et sensibiliser les utilisateurs :** déterminer les personnes qui sont habilitées à accéder aux données à caractère personnel ; supprimer les permissions d'accès obsolètes ; rédiger une charte informatique et l'annexer au règlement intérieur lorsqu'il en existe un.
- **sécuriser l'informatique mobile :** prévoir des moyens de chiffrement 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.
- **sauvegarder et prévoir la continuité d'activité :** mettre en place des sauvegardes régulières, stocker les supports de sauvegarde dans un endroit sûr, etc.

4. Comment notifier et communiquer sur une violation des données à caractère personnel ?

Veuillez vous reporter à la fiche suivante n° 9 « Procédure en cas de violation de données ».

À FAIRE	
Mettre en place des mesures de sécurité physiques :	☐
• Limiter l'accès au cabinet	☐
• Vérifier et sécuriser le lieu de stockage des dossiers	☐
• Installer et activer une alarme	☐
Mettre en place des mesures de sécurité logiques :	☐
• Installer des mesures d'authentification de l'utilisateur	☐
• Gérer les habilitations et sensibiliser les utilisateurs	☐
• Sécuriser l'informatique mobile	☐
• Sauvegarder et prévoir la continuité de l'activité	☐
Mettre en place une charte informatique	☐
Mettre en place des procédures de notification de violations de données personnelles	☐

En savoir plus : La CNIL a publié, en janvier 2018, un guide rappelant les précautions élémentaires qui devraient être mises en œuvre de façon systématique :

https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

FICHE N°9. PROCEDURE EN CAS DE VIOLATION DE DONNEES

Notification auprès de la CNIL. La violation de données à caractère personnel est une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Sauf dans les cas où la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, il conviendra de la notifier à l'autorité de contrôle compétente à savoir la CNIL dans les meilleurs délais et si possible, **au plus tard dans les 72 heures** après en avoir pris connaissance (RGPD , art. 33).

Cette notification doit, entre autres choses, préciser :

- la nature de la violation des données à caractère personnel (catégories et nombre approximatif de personnes et d'enregistrements de données concernés) ;
- Le nom et les coordonnées du DPO ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- les conséquences probables de la violation ;
- les mesures prises ou à prendre en vue d'atténuer les éventuelles conséquences négatives.
- Un formulaire de notification de violation de données à caractère personnel est à la disposition du responsable de traitement sur le site de la CNIL : https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf

Il est également recommandé de :

- mettre en place des mesures permettant d'analyser les risques du traitement mis en place pour les droits et libertés des personnes physiques ;
- s'assurer de notifier les violations dans un délai de 72 heures à défaut de quoi il devra fournir des explications sur ce retard à l'autorité de contrôle compétente dans l'Etat concerné ;
- indiquer dans la notification les faits concernant la violation, la nature de cette violation, ses effets ainsi que les mesures prises pour y remédier ;
- faire tous ses efforts afin de documenter au mieux toute violation pour permettre à l'autorité de contrôle de vérifier le respect des exigences imposées par le RGPD ;
- mettre en place des mesures d'urgence afin de pouvoir remédier à la violation et en atténuer les conséquences.

Si le cabinet d'avocats a un sous-traitant, celui-ci devra également notifier au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. Il est recommandé de le préciser contractuellement.

Communication auprès des personnes concernées. Il conviendra également, sauf dans les cas où la violation n'est pas susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, d'informer directement la personne concernée de la violation.

Cette communication ne sera pas nécessaire si :

- des mesures techniques et organisationnelles ont rendu les données incompréhensibles pour toute personne (ex. : chiffrement) ;
- des mesures ont été prises pour que le risque ne soit plus « susceptible de se matérialiser » ;

De plus, le RGPD autorise une communication « publique » plutôt que directe si la communication exige des « efforts disproportionnés ».

Si le cabinet d'avocats ne procède pas à la communication de la violation de données à la personne concernée, l'autorité de contrôle pourra, après avoir examiné le risque résultant de cette violation, enjoindre le responsable de traitement de procéder à cette communication.

À FAIRE	
Mobiliser les **personnes** compétentes	☐
Qualifier la violation	☐
Prendre les mesures nécessaires en vue d'atténuer les éventuelles conséquences	☐
Si risque : notification de la violation à la CNIL	☐
Si risque élevé : communication auprès des personnes concernées	☐
En tout état de cause, insertion au sein du registre des violations	☐

FICHE N°10. LE REGISTRE DES ACTIVITES DE TRAITEMENT

En contrepartie de la suppression des formalités déclaratives, le RGPD prévoit l'instauration d'un registre des activités de traitement qui doit être tenu par le responsable de traitement.

Chaque responsable de traitement devra tenir un registre des catégories de traitement de données à caractère personnel 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.

Il semble donc qu'un grand nombre de cabinets d'avocats, dès lors que leurs traitements portent sur des données relatives à des catégories particulières de données ou des données se rapportant à des condamnations et des infractions pénales, seront soumis à l'obligation de mettre en place un registre des activités de traitement.

En tout état de cause, même pour ceux qui n'y seraient pas obligés, la tenue d'un registre contribue au respect du principe d'accountability (consistant à documenter la conformité pour pouvoir la prouver) et, à ce titre, est vivement conseillée.

En effet, l'absence d'obligation de tenir un registre n'est pas un blanc-seing en matière de gestion des données personnelles, bien au contraire. Il convient a minima d'avoir une cartographie des traitements, de respecter tous les principes visés au RGPD, de respecter les droits des personnes et de documenter le respect de ces diverses obligations conformément au principe d'accountability.

Le registre doit, conformément à l'article 30 du RGPD, comporter les informations suivantes :

- Le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
- Les finalités du traitement ;
- Une description des catégories de données traitées, ainsi que les catégories de personnes concernées par le traitement ;
- Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou vers une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale, et les documents attestant de l'existence de garanties appropriées ;

- Dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.

À FAIRE	
Cartographier les traitements mis en œuvre au sein du cabinet	
• Recensement des traitements (gestion des dossiers clients, gestion des ressources humaines, gestion de la comptabilité, etc.)	☐
• Identification des caractéristiques de chaque traitement (données collectées, destinataires, durée de conservation, etc.)	☐
Élaboration du registre des activités de traitement	☐

FICHE N°11. LE DELEGUE À LA PROTECTION DES DONNEES

1. Obligation des cabinets d'avocats de désigner un délégué à la protection des données

Aux termes de l'article 37 du RGPD, les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué :

- S'ils appartiennent au secteur public ;
- Si leurs activités de base (principales) les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ;
- Si leurs activités de base (principales) les amènent à traiter (toujours à grande échelle) des catégories particulières de données, dites « sensibles », et des données relatives à des condamnations pénales et à des infractions ;

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible, et même recommandée.

Il n'existe pas de seuil en termes d'effectifs qui rend obligatoire la désignation d'un délégué à la protection des données.

Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe.

Le groupe de travail « Article 29 » (G29), composé de représentants des autorités de protection des données des États membres de l'UE, a publié des lignes directrices sur le rôle des délégués à la protection des données et a fourni des recommandations concernant les bonnes pratiques.

Si un délégué à la protection des données est désigné, l'organisation est tenue de publier les informations relatives au délégué à la protection des données et de les communiquer à l'autorité de contrôle compétente.

Néanmoins, l'article 37 (de même que l'article 35, voir ci-dessous) s'applique toujours au responsable du traitement ou au sous-traitant de catégories particulières de données. Ces dispositions exigent la désignation du délégué à la protection des données dans les cas où les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9.

Selon les lignes directrices sur les délégués à la protection des données, les *« activités de base peuvent être considérées comme l'ensemble des activités pour lesquelles le traitement de données fait partie intégrante des activités du responsable du traitement ou du sous-traitant ».*

La signification de l'expression *« à grande échelle »* revêt une importance particulière, dans la mesure où un petit cabinet d'avocats peut avoir à traiter des dossiers impliquant des quantités considérables de données.

Néanmoins, le considérant 91 du RGPD permet de soutenir facilement que cette exigence ne s'appliquera pas aux avocats qui exercent à titre individuel (voir le point 1.3.2.4 relatif à l'analyse d'impact).

Ainsi, l'appréciation de l'obligation de désigner ou non un délégué à la protection des données doit se faire au cas par cas, en fonction notamment du nombre de personnes concernées par les traitements de données à caractère personnel, du volume des données traitées, de la durée ou de la permanence des activités de traitement, de l'étendue géographique de l'activité de traitement mais il semble que, pour la plupart, les cabinets d'avocats ne peuvent être considérés comme effectuant des traitements de données à caractère personnel à grande échelle et que, dès lors, la désignation d'un délégué à la protection des données ne sera pas obligatoire

En tout état de cause, une telle désignation, même non obligatoire, devrait également s'analyser en opportunité dans la mesure où elle permettrait de désigner une personne pour se charger de la conformité du cabinet.

2. Obligations et missions du délégué à la protection des données

Le RGPD impose des obligations importantes aux délégués à la protection des données. « Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

- D'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- De s'assurer du respect du règlement et du droit national en matière de protection des données ;
- De conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- De coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci. Pour vous accompagner dans la mise en place des nouvelles obligations imposées par le règlement européen, le délégué doit notamment :
- S'informer sur le contenu des nouvelles obligations ;
- Sensibiliser les décideurs sur l'impact de ces nouvelles règles ;
- Réaliser l'inventaire des traitements de données de votre organisme ;
- Concevoir des actions de sensibilisation ;
- Piloter la conformité en continu.

En conséquence, la personne qui agit en tant que délégué à la protection des données endossera d'importantes responsabilités.

3. Avocat agissant en qualité de délégué à la protection des données

Opportunément, le RGPD a abrogé le seuil des 50 salariés qui interdisait d'externaliser le correspondant informatique et libertés (CIL).

La décision à caractère normatif portant réforme des articles 6 « Le champ d'activité professionnelle de l'avocat » et 19 « Prestations juridiques en ligne » du Règlement intérieur national (RIN) de la profession d'avocat, adoptée par l'assemblée générale du Conseil national des barreaux des 9 et 10 décembre 2016[6] sur la base d'un rapport de sa commission des règles et usages, et après concertation de la profession, a modifié les dispositions encadrant la mission d'avocat-CIL :

https://www.cnb.avocat.fr/reglement-interieur-national-de-la-profession-davocat-rin#

L'article 6.3.3 « Correspondant à la protection des données à caractère personnel – Correspondant Informatique et libertés (CIL) » du RIN prévoit désormais :

« L'avocat correspondant à la protection des données à caractère personnel doit mettre un terme à sa mission s'il estime ne pas pouvoir l'exercer, après avoir préalablement informé et effectué les démarches nécessaires auprès de la personne responsable des traitements ; en aucun cas il ne peut dénoncer son client.

L'avocat correspondant à la protection des données à caractère personnel doit refuser de représenter toute personne ou organisme pour lesquels il exerce ou a exercé la mission de correspondant à la protection des données à caractère personnel dans le cadre de procédures administratives ou judiciaires mettant en cause le responsable des traitements. »

A compter du 25 mai 2018, ces dispositions seront remplacées par les dispositions suivantes :

« 6.3.3 : Délégué à la Protection des Données.

L'avocat Délégué à la Protection des Données doit mettre un terme à sa mission s'il estime ne pas pouvoir l'exercer, après avoir préalablement informé et effectué les démarches nécessaires auprès de la personne responsable des traitements ; en aucun cas il ne peut dénoncer son client.

L'avocat Délégué à la Protection des Données doit refuser de représenter toute personne ou organisme pour lesquels il exerce ou a exercé la mission de correspondant à la protection des données à caractère personnel (CIL) ou de Délégué à la Protection des Données dans le cadre de procédures administratives ou judiciaires mettant en cause le responsable des traitements. »

L'avocat-CIL était déjà soumis à deux devoirs qui ne s'imposent pas au CIL non avocat : le devoir de non-dénonciation de son client et le devoir de démission en cas de conflit d'intérêts.

6. Publiée au Journal officiel du 13 avril 2017

Il est apparu nécessaire de préciser que l'avocat doit refuser de représenter les clients pour lesquels il exerce ou a exercé la mission de CIL dans les procédures mettant en cause le responsable des traitements, afin d'éviter toute situation de conflit d'intérêts ou de violation du secret professionnel.

Par ailleurs, l'article 6.4 « Déclarations à l'Ordre » du RIN dispose :

« L'avocat qui entend exercer l'activité de mandataire en transaction immobilière, en gestion de portefeuille ou d'immeubles, de mandataire sportif, de mandataire d'artistes et d'auteurs, d'intermédiaire en assurances, de lobbyiste, de syndics de copropriété et de Correspondant à la protection des données à caractère personnel – Correspondant Informatique et libertés (CIL) doit en faire la déclaration à l'Ordre, par lettre ou courriel adressée au Bâtonnier. »

A compter du 25 mai 2018, dans l'article 6.4, les mots *« Correspondant à la protection des données à caractère personnel Correspondant Informatique et libertés (CIL) »* sont remplacés par les mots *« Délégué à la Protection des Données ».*

Il s'agit d'une simple obligation de déclaration, sans contrainte formelle. Ainsi, cette déclaration vise d'une part à permettre une meilleure formation des avocats souhaitant les exercer, et d'autre part à permettre aux Ordres de communiquer sur les avocats exerçant ces misions dans leur ressort.

FICHE N°12. AUTORITE DE CONTROLE ET SANCTIONS

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 autorités de contrôle (en France, la CNIL) peuvent notamment :

- Prononcer un avertissement ;
- Mettre en demeure l'entreprise ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données.

S'agissant des nouveaux outils de conformité qui peuvent être utilisés par les entreprises, l'autorité peut retirer la certification délivrée ou ordonner à l'organisme de certification de retirer la certification.

S'agissant des amendes administratives, elles peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de **2% jusqu'à 4% du chiffre d'affaires annuel mondial,** le montant le plus élevé étant retenu.

Ce montant doit être rapporté au fait que, pour les traitements transnationaux, la sanction sera conjointement adoptée entre l'ensemble des autorités concernées, donc potentiellement pour le territoire de toute l'Union européenne.

Dans ce cas, une seule et même décision de sanction décidée par plusieurs autorités de contrôle sera infligée à l'entreprise.

FICHE N°13. DROIT D'ACCES AUX DONNEES

Le RGPD opère les changements suivants en matière de droit d'accès :

- **Les délais pour répondre à une demande :** le délai de réponse est désormais d'un mois maximum à compter de la réception de la demande (article 12.3). Cependant, une possibilité de prolonger de deux mois ce délai est prévue, « *compte tenu de la complexité et du nombre de demandes* », à condition d'en informer la personne concernée dans le délai d'un mois suivant la réception de la demande (article 12.3).
- **Les frais de reproduction :** le règlement prévoit un principe de gratuité pour les copies fournies dans le cadre d'une demande d'accès (article 12.5). Ce n'est que lorsque la demande est manifestement infondée ou excessive que le responsable de traitement pourra exiger le paiement de « frais raisonnables » qui tiennent compte des coûts administratifs supportés pour fournir les informations. Il en ira de même lorsqu'une copie supplémentaire est demandée.
- **Les modalités de la communication des données :** le règlement précise que si la personne présente sa demande par voie électronique, les informations demandées sont communiquées sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement (article 12.3).
- **Les modalités de la communication des données :** le règlement prévoit que le sous-traitant aide le responsable de traitement à s'acquitter de ses obligations en matière de droit d'accès (article 28 e). Par exemple : un employeur pourrait demander à son sous-traitant lui ayant fourni un dispositif de géolocalisation, son appui afin de fournir aux employés qui en feraient la demande, des données de géolocalisations « sous une forme accessible » ; lorsque le responsable de traitement ne dispose que d'une analyse des données, il pourrait se rapprocher du sous-traitant qui aurait conservé les données identifiantes.

MÉTHODOLOGIE DE MISE EN CONFORMITÉ

Méthodologie de mise en conformité

La CNIL a développé une méthodologie en six étapes afin de faciliter la mise en conformité des responsables de traitements. Ces six étapes correspondent à :

- La désignation d'un pilote ;
- La cartographie des traitements de données à caractère personnel ;
- La priorisation des actions à mener ;
- La gestion des risques ;
- L'organisation des processus en interne ;
- La documentation de la conformité.

1. La désignation d'un pilote

L'article 37 du RGPD a introduit l'obligation de désigner un délégué à la protection des données dans différentes hypothèses (nous vous invitons à vous référer à la Fiche N° 11).

Pour la majorité des cabinets d'avocats, il ne semble pas qu'une telle désignation soit obligatoire dès lors que, s'ils traitent des catégories particulières de données ou des données relatives aux infractions et condamnations, la plupart d'entre eux pourront soutenir ne pas traiter ces données « à grande échelle ».

Cependant, même dans les cas où la désignation du délégué à la protection des données, n'est pas obligatoire, la CNIL recommande une telle désignation afin de faciliter la mise en conformité au RGPD (voir la fiche n° 11).

Sans même désigner une personne qui aurait la qualité de délégué à la protection des données, il serait opportun de désigner parmi les membres du cabinet une personne chargée des aspects liés à la protection des données et qui servira de référent pour le personnel et les collaborateurs du cabinet.

2. La cartographie des traitements de données personnelles

Cette cartographie permet d'avoir une vue d'ensemble des traitements de données à caractère personnel opérés au sein du cabinet d'avocats.

La CNIL préconise donc de se poser les questions suivantes :

- Qui ?
- Quoi ?
- Pourquoi ?
- Jusqu'à quand ?
- Comment ?

Qui ? Cette question permet d'identifier les différents acteurs à savoir le responsable de traitement mais également les sous-traitants et les destinataires des données.

- **Responsable de traitement.** Au sein du cabinet d'avocats, le responsable de traitement est celui qui détermine la finalité et les moyens du traitement, il peut donc s'agir, entre autres, de l'avocat associé. Il convient à cet effet d'identifier la personne au sein du cabinet d'avocats qui est à l'initiative du traitement de données personnelles. Il peut également s'agir du cabinet lui-même en tant que personne morale.
- **Sous-traitant.** Le sous-traitant est la « personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement » selon l'article 4, alinéa 8, du RGPD. Il peut donc s'agir des prestataires, des fournisseurs, des éditeurs de logiciels, des hébergeurs, etc.
- **Destinataires.** Le RGPD définit à l'article 4, alinéa 9, le destinataire d'un traitement de données à caractère personnel qui est « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ».

Quoi ? Il s'agit ici de savoir quelles sont les données à caractère personnel que le cabinet collecte, et de manière plus générale traite. En outre, il appartient à l'avocat d'identifier la présence de catégories particulières de données à caractère personnel (les données de santé, les données concernant la vie sexuelle, les données relatives aux condamnations pénales et aux infractions, etc.).

Pourquoi ? Par cette question, l'avocat détermine la finalité du traitement de données à caractère personnel qu'il opère, c'est-à-dire l'objectif (par exemple : gestion clients, gestion des ressources humaines, gestion de la sollicitation personnalisée, etc.).

Où ? A ce stade, il s'agit de déterminer le lieu où sont stockées les données à caractère personnel (un serveur spécifique, en local, en partage ? Les dossiers sont-ils stockés dans une salle accessible à tout le cabinet d'avocat ? etc.). Cette question doit également permettre à l'avocat d'identifier les éventuels transferts de données vers des pays hors UE (un dossier international, un avocat postulant à l'étranger, etc.).

Quand ? Le cabinet d'avocat a-t-il mis en place une politique de conservation, d'archivage et de suppression des données ? Le cabinet d'avocat a-t-il prévu une purge des données qu'il collecte ?

Comment ? Le cabinet d'avocat doit identifier les mesures de sécurité physique et logique mises en place pour garantir la protection des données à caractère personnel qu'il collecte.

3. Identifier les actions prioritaires

Plusieurs actions peuvent être menées par le responsable de traitement afin de garantir la conformité de ses traitements au RGPD.

Le cabinet d'avocats devra donc déterminer s'il respecte :

- Le principe de minimisation c'est-à-dire qu'il ne traite que des données strictement nécessaires à la finalité de son traitement ;
- Le principe de licéité c'est-à-dire déterminer la base juridique du traitement de données personnelles mis en œuvre par le cabinet d'avocats (conclusion et exécution d'un contrat, nécessité de se conformer à une obligation légale, consentement, intérêt légitime etc.) ;
- L'obligation de mentions d'information (convention d'honoraires, contrat de travail, contrat de collaboration, site web, etc.) ;
- Les obligations contractuelles relatives aux sous-traitants (comptable, hébergeur du système d'information, prestataire informatique, éditeur de logiciel client ou de comptabilité par exemple) ;
- Les droits des personnes ;
- Les mesures de sécurité mises en œuvre dans le cabinet (accès au locaux, mots de passe, habilitations, etc.).

Attention, le cabinet d'avocats devra être vigilant en présence de données particulières et de données relatives aux condamnations pénales et aux infractions ainsi qu'en présence de flux transfrontières de données personnelles.

4. La gestion des risques

Cette étape vise la nécessité de réaliser une analyse d'impact. En effet, certains cabinets d'avocats, selon les données personnelles qu'ils collectent, pourraient être amenés à devoir réaliser des analyses d'impact.

Pour en savoir plus sur les analyses d'impact, veuillez vous référer au point 1.3.2.4.

5. La mise en place de processus de protection de données personnelles au sein du cabinet d'avocats

Les cabinets d'avocat peuvent mettre en place des processus afin de garantir la conformité de leurs traitements des données personnelles au regard du RGPD.

Parmi ces processus, il existe :

- La protection des données personnelles dès la conception et la sécurité par défaut ;
- La sensibilisation des membres du cabinet aux problématiques relatives à la protection des données personnelles ;

- Les modalités de gestion des demandes relatives aux différents droits des clients. En effet, plus le cabinet d'avocats réagit rapidement en faisant droit aux demandes de droit d'accès, d'opposition, de rectification, etc. du client, moins il y a de risques que celui-ci introduise une réclamation auprès de l'autorité de contrôle laquelle pourrait aboutir à un contrôle de sa part ;
- Les mesures internes relatives aux violations des données personnelles à savoir la notification à l'autorité de contrôle et la communication aux personnes concernées.

6. La documentation de la conformité

- Le cabinet d'avocats doit conserver des preuves de la conformité de ces traitements de données personnelles au regard du RGPD. Plusieurs outils sont disponibles afin de documenter la conformité de ses traitements :
- Le registre des traitements ;
- L'analyse d'impact ;
- Les outils d'encadrement des flux transfrontières tels que les clauses contractuelles types, les *Binding Corporate Rules*, les certifications, etc. ;
- Les mentions d'informations ;
- Les contrats avec les sous-traitants ;
- Les preuves du recueil du consentement des données personnelles.

POUR EN SAVOIR PLUS

Lignes directrices du G29 :

https://www.CNIL.fr/fr/reglement-europeen/lignes-directrices

- Délégué à la protection des données (5/05/2017)
- Analyse d'impact relative à la protection des données (DPIA) (4/10/2017)
- Portabilité (5/05/2017)
- Désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant (5/05/2017)

Lignes directrices du Conseil des barreaux européens (CCBE) sur les principales nouvelles mesures de conformité des avocats au RGPD (19/05/2017) :

http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/FR_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf

Guides d'information de la CNIL :

https://www.CNIL.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

https://www.CNIL.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

https://www.CNIL.fr/fr/video-le-youtubeur-cookie-connecte-repond-vos-questions-sur-larrivee-du-rgpd

Commission Européenne :

- Communication publiée le 24 janvier 2018 par la Commission au Parlement européen et au Conseil : Une meilleure protection et de nouvelles perspectives - Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 :

  http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52018DC0043

nouvel outil en ligne qui comprend des fiches pratiques, des Questions/réponses et des illustrations pratiques, destiné à aider les citoyens et les entreprises à se conformer aux nouvelles règles introduites par le règlement.

AUTRE TEXTE EN VIGUEUR

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil :

http://eurlex.europa.eu/legalcontent/FR/AUTO/?uri=uriserv:OJ.L_.2016.119.01.0089.01.FRA&toc=OJ:L:2016:119:TOC

Membres du groupe de travail constitué pour l'élaboration de ce guide :

Pour le Barreau de Paris :

Alexandra PERQUIN, MCO, présidente de la commission numérique

Cynthia de JAHAM, assistante ordinale, rattachée à la commission numérique

Pour le Conseil national des barreaux :

Sandrine VARA, présidente de la commission numérique

Dominique de GINESTET, présidente de la commission des règles et usages

Laurence DUPONT, juriste-adjointe à la directrice du Pôle juridique, Correspondant Informatique et libertés du CNB

Michel TRUONG, directeur des systèmes d'information

Pour la Conférence des Bâtonniers :

Philippe BARON, vice-président, ancien Bâtonnier du Barreau de Tours

Experts :

Anne RENARD, avocate au Barreau de Paris, directrice de l'activité Conformité et Certification du cabinet Lexing Alain Bensoussan Avocats

Anne-Laure VILLEDIEU, avocate au Barreau de Paris, directrice du pôle Nouvelles Technologies du cabinet CMS-Bureau Francis Lefebvre Avocats

Xavier LECLERC, Président, et **Martial Mercier,** Directeur général du groupe Anaxil-DPMS

Remerciements particuliers aux rédactrices de ce guide :

Anne RENARD, avocate au Barreau de Paris, directrice de l'activité Conformité et Certification du cabinet Lexing Alain Bensoussan Avocats

Laurence DUPONT, juriste-adjointe à la Directrice du Pôle juridique, Correspondant Informatique et libertés du CNB

Cynthia de JAHAM, assistante ordinale, rattachée à la commission numérique du Barreau de Paris

CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

1re édition | Mars 2018
Etablissement d'utilité publique
Art. 21-1 de la loi n°71-1130 du 31 décembre 1971 modifiée

180 Boulevard Haussmann - 75008 Paris
Tél. 01 53 30 85 60 - Fax. 01 53 30 85 62
www.cnb.avocat.fr
cnb@cnb.avocat.fr

Ce document à destination exclusive des avocats a été élaboré par le Conseil national des barreaux, le Barreau de Paris et la Conférence des Bâtonniers.