CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

AVOCATS BARREAU • PARIS

Conférence des Bâtonniers

GUIDE PRATIQUE
LES AVOCATS ET LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

2e ÉDITION
MAI 2023

SOMMAIRE

PRÉFACE DE LA PRÉSIDENTE DE LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS

©Juliette Coemelck

La protection des données constitue une préoccupation centrale pour la profession d'avocat tant l'avocat est amené à traiter chaque jour une quantité importante de données personnelles, souvent sensibles, assurant le double rôle de conseil et de garant de la confidentialité et de l'intégrité des données de ses clients. Fort de son expertise et de sa compréhension approfondie des enjeux éthiques et juridiques auxquels il est régulièrement confronté, l'avocat occupe une place particulière dans son approche de la conformité.

Entré en application en mai 2018, le RGPD a eu un impact considérable sur la manière dont les gouvernements, les entreprises et les professionnels collectent, traitent et stockent les données personnelles. Parue la même année, la première édition de ce guide a permis d'informer efficacement les avocats sur les bonnes pratiques à mettre en œuvre pour assurer la conformité de leurs traitements aux textes et aux lois en vigueur.

Depuis, le paysage de la protection des données n'a cessé d'évoluer, tant d'un point de vue normatif avec une abondante jurisprudence qui stabilise progressivement les contours du règlement, que d'un point de vue technique avec l'émergence de nouvelles technologies posant des défis inédits aux professionnels du droit.

Cette deuxième édition tient compte des évolutions et des enseignements tirés de ces cinq premières années de mise en œuvre du RGPD. Elle offre une vision actualisée et approfondie des concepts clés, des obligations et des bonnes pratiques à adopter dans le traitement des données personnelles. Je ne peux que me féliciter que le présent guide vise à capitaliser sur les productions de la Cnil en promouvant des pratiques respectueuses de la vie privée, tout en soutenant les avocats dans leur adaptation aux enjeux numériques actuels.

La nécessité de garantir le respect de la vie privée et le contrôle des informations personnelles est devenue incontournable, et les avocats jouent un rôle essentiel dans ce domaine. Votre expertise et votre compréhension approfondie des enjeux éthiques et juridiques vous placent au cœur de la protection des droits des personnes dans un monde de plus en plus axé sur les données. La Cnil reste engagée à vos côtés pour vous accompagner.

Marie-Laure Denis,
Présidente de la Commission nationale
de l'informatique et des libertés (Cnil)

AVANT-PROPOS

Le 27 mars 2018 était mis à la disposition des avocats un premier guide leur permettant d'appréhender l'arrivée du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit Règlement général sur la protection des données (RGPD).

Ce guide, élaboré conjointement par le Conseil national des barreaux, le Barreau de Paris et la Conférence des bâtonniers, était essentiel pour informer la profession des changements occasionnés par le texte européen, en application depuis le 25 mai 2018, les avocats étant particulièrement impactés compte tenu de la sensibilité des traitements qu'ils mettent en œuvre et des données qu'ils réutilisent dans leur quotidien professionnel.

Cinq ans jour pour jour après l'entrée en application du RGPD, les trois institutions proposent aux avocats la mise à jour de ce référentiel avec la publication d'une deuxième édition du guide dont le contenu a été relu par les services de la Commission nationale de l'informatique et des libertés (Cnil) qui doivent en être sincèrement remerciés. Remaniée et actualisée sur le fond, à partir notamment des travaux de la Cnil et du Comité européen de protection des données (CEPD, ou EDPB en anglais), cette nouvelle édition du guide est également accompagnée de plusieurs documents et registres types, obligatoires pour certains, mis à la disposition des cabinets afin de leur permettre d'assurer au mieux leur obligation de documentation de la conformité au RGPD.

Un autre enjeu de conformité est aussi celui de la sécurité des données personnelles à l'heure où les atteintes aux données explosent, essentiellement dues à des attaques informatiques toujours plus nombreuses et complexes et dont les conséquences peuvent s'avérer extrêmement critiques.

La deuxième édition du guide prend particulièrement en compte cette problématique et sensibilise tout spécialement les avocats aux risques cyber et à la maîtrise de ces risques.

La recherche d'une plus grande confidentialité en pratique des données traitées par les cabinets, et plus généralement le respect de l'ensemble des règles relatives à la protection des données, renforcent toujours un peu plus le lien entre les avocats et leurs clients et constituent un gage de sérénité et de sécurité juridique pour tous.

Julie Couturier,
Vice-présidente du Conseil national des barreaux,
Bâtonnière de l'Ordre des avocats du Barreau de Paris

Jérôme Gavaudan,
Président du Conseil national des barreaux

Bruno Blanquer,
Vice-président du Conseil national des barreaux,
Président de la Conférence des Bâtonniers

PARTIE I
CADRE GÉNÉRAL DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Le 25 mai 2018 entrait en application 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 [1], dit Règlement général sur la protection des données (RGPD), abrogeant de fait l'ancienne directive de l'Union européenne sur la question datant de 1995 (directive 95/46/CE).

Ce texte a renforcé les droits existants en matière de protection des données à caractère personnel pour les personnes physiques afin de garantir que le traitement de leurs données soit suffisamment sécurisé, de garder le contrôle sur leurs données et de s'assurer que ce traitement ne génère pas de risques excessifs pour les droits et libertés de ces personnes. Il a aussi renforcé les obligations et la responsabilité des organisations qui traitent des données à caractère personnel.

Bien qu'il soit d'application directe et notamment des dérogations et spécificités nationales prévues en son sein, le RGPD a été intégré dans une réforme de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [2], dite « loi Informatique et libertés », effective au 1er juin 2019 *via* son décret d'application (décret n°2019-536 du 29 mai 2019). La refonte de la loi Informatique et libertés a aussi transposé la directive n°2016/680 du 27 avril 2016 [3], dite directive Police-Justice (qui établit des règles relatives 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces).

Le RGPD s'applique à tous les cabinets d'avocats, quels que soient leur taille, leur structure et leur domaine d'activité et il ne concerne que les données des personnes physiques, notamment les données considérées comme « sensibles » (cf. *infra*).

Le RGPD s'applique entre autres pour les personnes dont les données sont traitées par les cabinets d'avocats établis en France ou dans un autre État membre de l'Union européenne, et ce quelle que soit la nationalité des personnes concernées et que le traitement ait lieu ou non au sein de l'Union (notamment dans le cadre d'inscription dans un barreau étranger, d'une activité connexe ou d'un établissement secondaire).

1. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679.
2. https://www.legifrance.gouv.fr/loda/id/LEGISCTA000006095896.
3. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016L0680.

1. LA PROTECTION DES DONNÉES PERSONNELLES, UN ENJEU ET UN ATOUT POUR LES AVOCATS

Les données à caractère personnel traitées par les avocats sont principalement celles de leurs clients, mais les traitements peuvent aussi concerner les collaborateurs, salariés, fournisseurs et prestataires du cabinet, etc.

Les données auxquelles les avocats ont accès dans l'exercice de leur profession relèvent très souvent de la vie privée des clients personnes physiques ou des autres personnes concernées par un dossier, notamment les adversaires[4] : situation familiale, situation financière ou patrimoniale, santé des personnes, condamnations pénales, opinion politique ou religieuse, orientation sexuelle, lieu de résidence, données concernant des mineurs, etc. Certaines de ces informations sont considérées *a minima* comme « hautement personnelles[5] », voire « sensibles[6] ». Plus généralement, l'avocat traite des données à caractère personnel qui peuvent aussi affecter la vie professionnelle, la carrière et la réputation des personnes concernées.

C'est pourquoi le professionnel doit être particulièrement vigilant et exigeant en termes de sécurité dans le traitement de ce type d'informations ; en effet, une divulgation ou un accès non autorisé(e) à ces données pourrait porter atteinte aux droits et libertés des personnes concernées et se révéler critique pour ces dernières.
Cette vigilance accrue est d'ailleurs totalement complémentaire avec l'attention particulière que l'avocat porte déjà aux informations traitées pour le compte de ses clients.

De la sorte, l'application du RGPD est en totale adéquation avec la protection du secret professionnel et le respect des obligations déontologiques de l'avocat, et tous trois participent à l'accroissement du lien de confiance qui doit exister entre l'avocat et son client. De surcroît, le respect de ces éléments, notamment dans l'univers du numérique, participe pour les avocats à **développer leur cabinet et asseoir leur transformation numérique sans perdre leurs valeurs et la confiance de leurs clients.**

Le respect de la réglementation applicable à la protection des données et de la réglementation propre à la profession d'avocat est ainsi un gage de sécurité juridique.

4. Également, les représentants et mandataires du client personne morale, les employés du client ou du groupe du client (dans un dossier de droit social par exemple), les employés ou représentants d'un partenaire commercial du client, les clients du client (comme les consommateurs), etc.
5. L'expression de « données à caractère hautement personnel » est citée dans les **lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) [...]** éditées par le Comité européen de protection des données (CEPD). À titre d'exemple, les données financières sont considérées comme des données hautement personnelles (**délibération de la Cnil du 6 septembre 2018**), tout comme les données de (géo)localisation (**délibération de la Cnil du 16 mars 2023**).
6. Légalement dénommées « catégories particulières de données » à l'**article 9 du RGPD**.

2. GLOSSAIRE

- ***Analyse d'impact relative à la protection des données (ou étude d'impact – PIA) :*** outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée. L'AIPD concerne les traitements de données personnelles qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées, au sens de l'article 35 du RGPD[7] (voir le point 3.2 de la partie I).
- ***Comité européen de la protection des données (CEPD, en anglais EDPB) :*** regroupant les chefs des autorités de contrôle de chaque État membre de l'Union européenne ainsi que le Contrôleur européen de la protection des données (aussi désigné CEPD ou anglais EDPS) ainsi que les autorités de contrôle des États de l'Espace économique européen en ce qui concerne les questions liées au RGPD, mais sans droit de vote, le CEPD a pour mission de veiller à l'application cohérente du RGPD. Pour ce faire, il adopte des documents d'orientations générales (lignes directrices, recommandations et bonnes pratiques) afin de clarifier les dispositions des actes législatifs européens en matière de protection des données et, de cette manière, fournir aux acteurs concernés une interprétation cohérente de leurs droits et obligations. Il prend aussi des décisions contraignantes pour trancher les différends entre autorités de contrôle qui lui seraient soumis. Le CEPD remplace l'ancien groupe de travail « article 29 » (G29) ayant déjà produit bon nombre de référentiels.
- ***Commission nationale de l'informatique et des libertés (Cnil) :*** autorité administrative indépendante, créée par la loi Informatique et libertés. Dans le cadre du RGPD, la Cnil est une autorité nationale de contrôle chargée de veiller à la protection des données à caractère personnel contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés.
- ***Délégué à la protection des données (DPD), aussi appelé* data protection officer *(DPO) :*** le DPO est chargé de veiller en interne à la conformité d'un organisme à la réglementation relative à la protection des données personnelles et de conseiller en ce sens une société ou une administration. La désignation d'un DPO est obligatoire dans certaines situations et fortement recommandée dans d'autres. Un avocat peut accomplir les missions de délégué à la protection des données.
- ***Destinataire (des données) :*** personne physique ou morale, autorité publique, 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 mais comme des « tiers autorisés[8] ».

7. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article35
8. Sur ce sujet, un **guide et un recueil de procédures** ont été publiés par la Cnil.

- ***Donnée à caractère personnel (ou donnée personnelle) :*** toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »). Une « personne physique identifiable[9] » peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification (de type CNBF), une adresse postale ou électronique, une date de naissance, un identifiant en ligne, etc.

  A contrario, les données d'une personne morale ou des données totalement anonymisées ne seront pas considérées comme des données à caractère personnel.
- ***Droits des personnes concernant leurs données :*** incluent notamment les droit à l'information, droit d'accès, droit de rectification, droit à la portabilité, droit d'effacement et droit d'opposition portant sur des données personnelles, droit à la limitation du traitement, droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, droit de définir des directives relatives au sort des données après la mort et droit d'introduire une réclamation devant une autorité de contrôle comme la Cnil (voir notamment le point 3.1.5 de la partie I).
- ***Loi Informatique et libertés (LIL) :*** loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que modifiée, qui est accompagnée d'un décret d'application, le décret n°2019-536 du 29 mai 2019.
- ***Personne concernée :*** personne à laquelle se rapportent les données personnelles qui font l'objet d'un traitement (cf. *supra*).
- ***Responsable du traitement :*** personne physique ou morale, autorité publique, service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement (le « pourquoi » et le « comment » d'un traitement).
- ***Sous-traitant :*** personne physique ou morale, autorité publique, service ou tout autre organisme qui traite des données à caractère personnel sur instruction et pour le compte du responsable du traitement.
- ***Traitement (de données) :*** 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.
- ***Violation de données personnelles :*** violation de 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 (voir le point 3.2 de la partie II).

Pour plus de définitions, veuillez consulter le **glossaire de la Cnil** en ligne.

9. Article 4.1 du RGPD.

3. LES PRINCIPES DE PROTECTION DES DONNÉES PERSONNELLES

Le Règlement général sur la protection des données a été élaboré de façon à s'adapter aux innovations technologiques et a harmonisé dans le même temps les législations nationales des États membres de l'Union européenne.

En pratique, le RGPD :

- est venu réaffirmer les principes fondamentaux de la protection des données datant de près d'un demi-siècle, notamment en renforçant les droits des personnes concernées par les traitements de données et en en créant de nouveaux (droit à la limitation du traitement, droit à l'oubli, droit à la portabilité des données à caractère personnel, création de dispositions propres aux personnes mineures, etc.) ;
- a introduit des concepts d'autonomie et de responsabilisation des acteurs (à savoir les responsables de traitement et sous-traitants) pour la mise en œuvre de leurs traitements, de documentation de leur conformité au RGPD et de gestion des risques, principalement de sécurité ;
- a renforcé la régulation grâce à des mesures de coopération entre les autorités de protection des données, qui pourront notamment adopter des mesures répressives conjointes et des décisions communes lorsque les traitements de données sont transnationaux.

Il s'agit d'un texte de « conformité » (en anglais *compliance*), qui exige la mise en place de processus, politiques internes et mesures de protection, d'une transparence vis-à-vis des personnes concernées et des autorités et plus généralement l'adoption d'une éthique.

3.1. Des principes fondamentaux renforcés ou créés par le RGPD

3.1.1. Finalité de traitement

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.

La question posée est l'objectif du traitement (« pourquoi » l'avocat détient-il telle ou telle donnée à caractère personnel concernant son client ou ses collaborateurs?). Les données collectées et traitées doivent ainsi obligatoirement répondre à un objectif précis et licite, formulé à l'avance.

Toute utilisation des données pour un objectif différent de celui qui avait été prévu avant la collecte initiale des informations (détournement de finalité) est passible de cinq ans d'emprisonnement et de 300 000 € d'amende (article 226-21 du Code pénal [10]).

10. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417981

Licéité du traitement (détermination d'une base légale). Sous réserve des dispositions spécifiques s'appliquant à certains types de données personnelles, l'article 6 du RGPD [11] dispose que le traitement de données personnelles doit se fonder sur l'une des six bases légales prévues, à savoir :

- le consentement de la personne concernée : par exemple dans le cas de transmission de prospection commerciale à des particuliers non clients du cabinet ;
- l'exécution du contrat ou de mesures précontractuelles : par exemple concernant la gestion des dossiers des clients (convention d'honoraires notamment) ;
- l'obligation légale : par exemple concernant les déclarations préalables d'embauche pour les salariés du cabinet ;
- la sauvegarde des intérêts vitaux de la personne ;
- l'exécution d'une mission d'intérêt public par le responsable de traitement : par exemple concernant la gestion de l'aide juridictionnelle ;
- l'intérêt légitime du responsable de traitement : par exemple dans le cas de transmission de *newsletters* d'information aux clients ou encore le déploiement de caméras de vidéosurveillance au sein du cabinet.

D'autres bases juridiques s'appliquent dans certains cas, et notamment en cas de catégories particulières de données (article 9 du RGPD), de données relatives aux condamnations pénales et aux infractions (article 10 du RGPD [12]) ou du numéro national d'identification (article 87 du RGPD [13]).

La détermination de la base légale du traitement est importante car elle entraîne un certain nombre de conséquences, et parmi elles :

- les droits RGPD (voir le point 3.1.5) activables par les personnes concernées ne seront pas les mêmes (par exemple, il ne pourra être répondu favorablement à une demande d'effacement, sauf exceptions [14], ou d'opposition sur des données si leur traitement est fondé sur une obligation légale) ;
- spécifiquement, le consentement pour une personne à voir ses données traitées comme base légale induit la conservation par le responsable de traitement de la preuve d'un consentement donné ou refusé et la réversibilité possible du choix initial, à tout moment, pour la personne concernée et dans les mêmes conditions.

NOTA : il n'est pas toujours possible de choisir à loisir la base légale correspondant à un traitement, un fondement juridique s'imposant souvent à une situation et par exclusion de toutes les autres ; tandis que si plusieurs bases peuvent s'appliquer à un traitement, un seul fondement doit être retenu sans possibilité de cumul (le CEPD énonce ainsi que « *l'application de l'une [des] six bases juridiques doit être établie avant l'activité de traitement et en lien avec une finalité spécifique* ») [15].

11. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article6
12. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article10
13. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre9#Article87
14. Si les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière, ou si les données ont fait l'objet d'un traitement illicite, ou si les données doivent être effacées pour respecter une obligation légale prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis.
15. Lignes directrices sur le consentement [...], p. 29.

3.1.2. Minimisation (proportionnalité et pertinence)

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

Il convient ainsi :

- de s'interroger sur l'absolue nécessité de collecter ou traiter chaque donnée à caractère personnel pour atteindre les finalités recherchées par le traitement ;
- si le traitement de données à caractère personnel s'avère nécessaire, de limiter le traitement des données au minimum en ce qui concerne :
  - les catégories de données traitées,
  - et le volume ou la quantité de données traitées.

Exemple 1 : il n'est pas utile d'enregistrer dans la base de données du cabinet des informations sur l'entourage familial d'un client lorsque, au regard des finalités du traitement et de la nature de l'affaire traitée, seuls sont nécessaires des éléments relatifs à sa vie professionnelle.

Exemple 2 : lorsque le client transmet par e-mail ou voie postale à l'avocat des documents contenant des données personnelles non nécessaires pour le traitement du dossier, il est fortement conseillé de retourner au client ces documents et/ou de les supprimer définitivement et d'en aviser le client.

NOTA : toute donnée déjà enregistrée et stockée qui ne serait pas finalement nécessaire au traitement doit être immédiatement purgée et, pour l'avenir, la collecte du même type d'information doit tout bonnement être arrêtée.

3.1.3. Conservation limitée des données

Les informations personnelles figurant dans un fichier ne peuvent être conservées indéfiniment. Une durée de conservation des données doit être établie en fonction du type de données enregistrées et de la finalité de chaque fichier, de manière cohérente et justifiée.

Dans certains cas, la durée de conservation minimum est fixée par la réglementation. Exemple : un avocat employeur doit conserver en vertu de l'article L. 3243-4 du Code du travail [16] « un double des bulletins de paie des salariés ou les bulletins de paie remis aux salariés sous forme électronique pendant cinq ans » et doit garantir en vertu de l'article D. 3248-8 du même Code la disponibilité de ce bulletin émis sous forme électronique soit pendant une durée de 50 ans soit jusqu'aux 75 ans présumés du salarié.

Néanmoins, pour de nombreux traitements, la durée de conservation des données n'est pas énoncée par un texte.

Dans ce cas, l'avocat responsable de traitement peut, pour déterminer la durée de conservation applicable, s'appuyer sur les différents outils d'aide à l'identification des durées élaborés par les délibérations de la Cnil ou les règles professionnelles.

16. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000020625846

En l'absence de tout élément en la matière, il appartient à l'avocat d'analyser le traitement opéré au cas par cas afin de fixer une durée de conservation raisonnable et en adéquation avec l'objectif de base (le temps de réalisation de la finalité). Souvent, le choix est effectué en considération du délai de prescription des actions pouvant résulter du document ou du traitement en question.

Attention : l'avocat devra toujours pouvoir justifier la raison de la conservation des données au-delà d'un délai fixé en cas de contrôle de la Cnil.

La Cnil a publié un **guide** spécifiquement consacré au principe de limitation de la durée de conservation et aux règles de conservation/archivage des données.
Pour en savoir plus concernant la durée de conservation et l'archivage des données du cabinet, il est renvoyé à l'annexe « Référentiel de durées de conservation des données et documents du cabinet » ainsi qu'à la fiche n°2 « La gestion des archives ».

3.1.4. Sécurité et confidentialité des données

L'avocat, en qualité de responsable du traitement, est astreint à une obligation générale de sécurité et de confidentialité portant sur les données personnelles sous sa responsabilité : il doit ainsi prendre toutes les mesures nécessaires pour garantir la confidentialité des données et éviter toute divulgation d'informations.

L'avocat prendrait un risque eu égard à sa responsabilité s'il était reconnu, par exemple à la suite d'un incident de sécurité, que l'avocat n'avait pas mis en œuvre les mesures nécessaires pour sécuriser les informations personnelles de ses clients, collaborateurs, salariés, etc, et/ou n'avait pas suffisamment adapté son niveau de sécurité à la sensibilité du traitement et des données en question (sensibilité généralement élevée du fait de l'activité de l'avocat).

En outre, dans le cas d'un incident de sécurité affectant les données et dont les conséquences présenteraient des risques pour les droits et libertés des clients, des collaborateurs, des salariés, etc., l'avocat a l'obligation de procéder à une notification de violation de données auprès de l'autorité de contrôle (la Cnil) et dans certains cas auprès de la ou des personne(s) concernée(s) directement (voir le point 3.2 de la partie II).

La Cnil a publié un **guide** complet sur la sécurité des données personnelles, accessible également sous forme de **minisite Internet**.
Pour en savoir plus concernant la sécurité et la confidentialité des données, il est renvoyé à la fiche n°6 « Les bonnes pratiques en termes de sécurité des données ».

3.1.5. Droits des personnes physiques concernées

À partir du moment où des données personnelles sont collectées et traitées par l'avocat, responsable de traitement, les personnes concernées (clients, collaborateurs libéraux ou salariés, associés, prestataires, etc.) disposent d'un certain nombre de droits afférents à leurs données afin qu'elles puissent garder le contrôle et la maîtrise sur leurs informations personnelles.

Face à une personne demandant l'exercice de ses droits, en application des articles 15 à 22 du RGPD [17], l'avocat responsable de traitement devra répondre au maximum dans un délai **d'un mois à compter de la réception de la demande.**
Ce délai pourra être prorogé de deux mois eu égard à la complexité de la demande et du nombre des demandes.

NOTA : dans une telle hypothèse, l'information de la prorogation et le motif de l'allongement du délai de réponse doivent être communiqués à la personne concernée avant la fin du délai initial (article 12.3 du RGPD).

Attention : compte tenu des spécificités de la profession d'avocat et du respect du secret professionnel, l'exercice de ces droits n'est ici pas absolu, et ce pour protéger les droits des tiers. De manière notable, l'avocat n'aura ainsi pas à faire droit à une demande émanant de la partie adverse ou d'un employé du client ou d'une société de son groupe. Dans la plupart des cas, l'avocat se trouvera dans l'impossibilité de commenter l'existence même de la relation d'affaires avec le client ou d'un dossier qui contiendrait les données de la personne à l'origine de la demande.

3.1.5.1. Le droit à la transparence (droit à l'information)

Le RGPD pose l'obligation d'informer les catégories de personnes concernées à partir du moment où un responsable de traitement traite leurs données à caractère personnel.

Le droit à l'information est peut-être le plus important des droits des personnes car il conditionne l'exercice de l'ensemble des autres droits ; en effet, si les personnes ignorent les finalités pour lesquelles (et la façon dont) le responsable de traitement traite leurs données, elles ne seront pas en mesure d'exercer leurs droits sur ces dernières [18].

Les informations sont à apporter par l'avocat « au moment où les données sont obtenues » et seront différentes selon que la collecte est effectuée directement ou non auprès de la personne concernée.

Lorsque les données personnelles ont été collectées directement auprès de la personne concernée, l'article 13 du RGPD dispose que les informations suivantes doivent être fournies au client, fournisseur, collaborateur ou salarié du cabinet :

- 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 (voir le point 4 de la partie II) ;
- 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 ;

17. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3
18. **Nota :** les notes d'informations ne nomment pas les personnes concernées, ces dernières pouvant continuer à ignorer que leurs données soient traitées.

- les destinataires ou les catégories de destinataires des données à caractère personnel ;
- 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.

Concrètement, ces informations pourront être portées au plus tard à la connaissance du client lors de la signature de la convention d'honoraires, du collaborateur ou salarié lors de la signature d'un contrat, ou encore de prospects dans une politique de confidentialité directement accessible sur le site Web du cabinet (voir la fiche n°9 « La mise en conformité du site Internet »). Pour autant, il n'est pas obligatoire de procéder à une information propre à chaque dossier mais plutôt sur les traitements effectués de façon générale par l'avocat.

A contrario, lorsque les données personnelles n'ont pas été collectées directement auprès de la personne concernée, l'article 14 du RGPD dispose que l'ensemble des informations prévues à l'article 13 soit porté à la connaissance de la personne concernée mais également :

- les catégories de données à caractère personnel concernées ;
- 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.

L'obligation d'information en cas de collecte indirecte pourrait donc s'appliquer par exemple en cas de transmission, dans le cadre d'un dossier, d'informations sur la partie adverse par le client à l'avocat ou encore en cas d'information sur un employé d'un client. Mais une telle communication poserait difficulté à l'avocat qui serait obligé d'informer la partie adverse de la constitution du dossier 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 fondée sur l'obligation légale de secret professionnel.

Enfin, au-delà du fond, la forme du droit d'information doit aussi être prise en compte : outre le fait que, pour rappel, les informations mentionnées doivent être communiquées au moment de la collecte des données, elles doivent être repérables facilement (page de données personnelles dédiée sur le site Internet du cabinet disponible par exemple en pied de page de chaque page du site, affichette présente au sein des locaux du cabinet et visible des clients lors d'un premier rendez-vous, rappel des informations au sein des dispositions contractuelles de la convention d'honoraires, etc.) et être suffisamment compréhensibles (vocabulaire et style d'expression simples ou adaptés au public cible, sommaire détaillé, choix d'intitulé clair, paragraphe aéré, etc.).
Pour matérialiser au mieux les obligations énoncées, il est renvoyé à l'annexe « Modèles de mentions d'information » ainsi qu'aux modèles (conventions d'honoraires, contrats de collaboration, etc.) publiés sur les espaces numériques édités par le Conseil national des barreaux.

3.1.5.2. Le droit d'accès

Toute personne physique, dont l'identité peut être prouvée, a le droit d'interroger un avocat, responsable d'un traitement de données à caractère personnel, pour lui demander s'il détient des informations la concernant et, dans l'affirmative, lui en demander une copie.

Cependant, afin d'éviter une violation du principe du secret professionnel, l'exercice du droit d'accès n'est pas absolu : une demande d'accès à des données exercée par la partie adverse ou toute autre personne physique concernée par un dossier (autre que le représentant légal du client) ne pourra être satisfaite par le cabinet d'avocats car les données traitées sont protégées dans le cadre de ce secret.

Pour en savoir plus concernant les modalités de réponse, il est renvoyé à la fiche n°11 « La gestion du droit d'accès aux données des personnes concernées ».

3.1.5.3. Le droit de rectification

Toute personne physique peut demander à l'avocat, responsable du traitement, que ses données soient, selon les cas, rectifiées, complétées, mises à jour, etc.

Sous les mêmes réserves de confidentialité et de défense des droits et intérêts du client propre à la profession, le droit de rectification remplit ainsi la fonction d'éviter toute utilisation de données obsolètes, inexactes ou incomplètes, notamment en cas de diffusion de ces données (par exemple lors d'une transmission d'un dossier).

3.1.5.4. Le droit d'opposition

Toute personne physique a le droit de s'opposer pour un motif légitime à ce que des données la concernant soient traitées.

Ici encore, l'exercice du droit d'opposition n'est pas absolu, l'avocat peut ainsi ne pas faire droit par exemple à une demande d'opposition d'une personne physique concernée par un dossier qui demanderait à faire cesser l'utilisation de ces données si un texte de loi rendait obligatoire ce traitement de données.

NOTA : en matière de prospection, le droit d'opposition peut être exercé sans motif (par exemple une demande de suppression d'une liste de diffusion pour des envois de *newsletters*) par les personnes physiques concernées. L'avocat doit alors dans ce cadre stopper l'utilisation dans les plus brefs délais de l'adresse électronique de la personne démarchée qui ne souhaite plus l'être, les systèmes actuels de gestion de *mailing list* écartant généralement instantanément les références d'une personne à des fins de prospection.

3.1.5.5. Le droit à l'effacement (droit à l'oubli)

Toute personne physique a le droit de demander l'effacement de ses données notamment si les informations personnelles ont été traitées de manière illicite ou si l'objectif pour lequel elles ont été collectées a été atteint.

Attention : l'effacement irréversible des données d'un dossier ne pourra pas par exemple être mis en œuvre avant l'expiration notamment de la durée de prescription de la responsabilité civile professionnelle de l'avocat[19] (il en va d'ailleurs de même pour toute autre prescription ou obligations, notamment fiscales ou en matière de LCB-FT).

3.1.5.6. Le droit de limitation

Toute personne physique a le droit de demander la limitation du traitement de ses données, c'est-à-dire le gel temporaire de l'utilisation de ses informations pendant le temps de réponse à une demande de rectification ou d'opposition (cf. *supra*).

Le droit de limitation est aussi utile en cas de conservation à des fins probatoires des données par l'avocat, données que la personne concernée souhaite voir effacées. Dans ce cadre, sous les mêmes réserves de confidentialité et de défense des droits et intérêts du client propre à la profession, la demande de limitation permet le marquage des données conservées pendant une période définie pendant laquelle les informations personnelles de la personne concernée ne pourront pas être traitées mais continuer à être conservées.

3.1.5.7. Le droit à la portabilité

Toute personne physique peut demander à récupérer les données personnelles qu'elle a fournies dans un format lisible par une machine (par exemple le langage JSON).

19. Article 17.3.e du RGPD.

Concrètement, l'avocat qui a reçu directement d'une personne physique ses données à caractère personnel est tenu de lui transmettre ses données à sa demande ou de les communiquer à un tiers lorsque le traitement initial repose sur l'un des fondements suivants :

- la personne concernée a exprimé son consentement au traitement de ses données à caractère personnel ou le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée (en dehors de la situation du client personne physique, il est très peu probable que ces fondements s'appliquent dans les dossiers traités pour les clients) ;
- et le traitement est effectué à l'aide de procédés automatisés (informatiques).

Concrètement, le droit à la portabilité des données personnelles fournies par un client personne physique pourra être mis en œuvre pour un avocat dans le cadre de la **succession d'avocats dans un même dossier.**

3.2. Responsabilisation des acteurs, documentation de la conformité et maîtrise des risques

Les organismes doivent non seulement assurer une protection optimale des données à chaque instant et respecter les obligations qui leur incombent, mais aussi être en mesure de démontrer à tout moment l'existence de cette protection et ce respect en documentant leur conformité : cette logique de responsabilisation (ou redevabilité) et d'obligation de documenter sa conformité est ce que l'on nomme l'*accountability* .

Ainsi, l'avocat doit être en mesure de démontrer à tout moment la conformité à la réglementation relative à la protection des données personnelles de ses traitements et le respect des principes de protection des données à caractère personnel dont il a la responsabilité, notamment par l'entremise de plusieurs documents ou procédures de conformité. Cette responsabilisation passera aussi par le respect de certaines mesures imposées par le RGPD (voir la partie II « Mise en conformité du cabinet ») :

- prendre en compte le principe d'*accountability* qui impose d'être en mesure de justifier l'ensemble des dispositifs de contrôle et d'encadrement mis en place pour assurer la conformité Informatique et libertés. La documentation de la conformité passe notamment par la tenue de trois documents :

  - le registre des activités de traitement : le RGPD impose aux avocats, en tant que responsables de traitement, de tenir un registre des activités de traitement effectuées sous leur responsabilité [20].
    À cet égard, il est renvoyé au point 3.1 de la partie II « Mise en conformité du cabinet » ainsi qu'à l'annexe « Registre type des activités de traitement en tant que responsable de traitement (article 30 du RGPD) ».

20. La Cnil a élaboré et publié sur son site Internet des modèles de registre de traitements : https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

  - le registre des activités de traitement en tant que sous-traitant : par principe, l'avocat ne peut pas être considéré comme un sous-traitant, sauf cas exceptionnels où l'avocat serait alors tenu de consigner les traitements correspondants dans un registre distinct du principal en tant que responsable de traitement. La tenue éventuelle de ce registre s'effectue dans les mêmes conditions que pour le précédent,
  - la documentation des violations de données : un avocat pourra malheureusement être confronté tout au long de son exercice professionnel à des incidents de sécurité touchant les données personnelles (accès illégitime, divulgation non autorisée, perte d'informations) sous sa responsabilité, de nature plus ou moins grave. Si certains d'entre eux nécessiteront une communication en externe et une information de certains acteurs (cf. *infra*), chacune des violations de données, même si elle ne présente aucun risque pour les personnes concernées, doit être consignée dans un document, ce dernier pouvant prendre par exemple la forme d'un registre dédié[21]. À cet égard, il est renvoyé au point 3.2 de la partie II « Mise en conformité du cabinet » ainsi qu'au modèle de registre de violations de données en annexes ;

- intégrer les concepts de protection des données à caractère personnel dès la conception (*privacy by design*) et par défaut (*privacy by default*)[22] en prenant en compte les impératifs demandés dans toutes les technologies exploitant des données à caractère personnel. Ainsi, l'obligation consiste essentiellement en la prise de mesures appropriées et la vérification de garanties nécessaires pour assurer, dès la conception et par défaut, la mise en œuvre effective des principes de protection des données et, par conséquent, des droits et libertés des personnes concernées ;
- identifier les risques pour la vie privée des personnes concernées engendrés par les traitements sous sa responsabilité et prendre toute mesure permettant de les réduire en renforçant la réponse en fonction du degré de dangerosité et de sensibilité du traitement (approche par les risques) ;
- notifier à la Cnil toute violation de données à caractère personnel en cas de risque pour les droits et libertés des personnes concernées (article 33 du RGPD) et communication de cette violation auprès de ces personnes en cas de risque élevé (article 34 du RGPD)[23]. Les notifications et communications effectuées doivent être documentées (voir le point 3.2 de la partie II) ;
- désigner un délégué à la protection des données (ou *data protection officer* - DPO), obligatoire pour quelques cabinets d'avocat, et le déclarer à la Cnil (voir le point 4 de la partie II) ; à défaut d'un DPO proprement dit, il est recommandé que les cabinets d'avocats aient recours à l'assistance d'un spécialiste pour les accompagner dans leur mise en conformité ;

21. Le CEPD conseille de longue date la tenue d'un registre, mais la forme de la documentation est laissée à la libre appréciation du responsable de traitement ; partant, les incidents de sécurité pourraient parfaitement être inscrits au registre des activités de traitement pour peu que les « informations concernant les violations soient clairement identifiables en tant que telles et puissent être extraites sur demande » (**Lignes directrices sur la notification de violations de données à caractère personnel en vertu du règlement (UE) 2016/679** mises à jour le 28 mars 2023, p. 26).

22. **Lignes directrices relatives à [la] protection des données dès la conception et protection des données par défaut.**

23. Sur ce sujet : **Lignes directrices sur la notification de violations de données à caractère personnel** (2018)
- Exemples concernant la notification de violations de données à caractère personnel (2021),
- Lignes directrices sur la notion de violation de données personnelles au sens du RGPD (2023, version anglaise).

- vérifier la conformité au RGPD de ses sous-traitants et, aux termes de l'article 28 du RGPD, s'assurer par exemple que son prestataire informatique a mis en place des mesures techniques et organisationnelles adaptées lui permettant de respecter la sécurité et la confidentialité des données. De surcroît, 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 (voir la fiche n°4 « La gestion des fournisseurs et prestataires » ainsi que le modèle de clauses de sous-traitance en annexe) ;
- obtenir une certification à une norme ISO existante, telle que la 27001, ou ne faire appel si possible qu'à des prestataires normés en ce sens (la norme ISO 27001 est utile notamment pour démontrer que le cabinet d'avocats présente un certain niveau de maturité et de prise en compte de la sécurité et la protection des données, bien qu'il ne s'agisse pas d'une « certification » au sens de l'article 42 du RGPD) ;
- recenser les éventuels transferts de données personnelles hors de l'Union européenne, notamment *via* les sous-traitants du cabinet, et vérifier que ces premiers sont bien encadrés par les différents outils juridiques disponibles (articles 45 à 49 du RGPD) et s'assurer que les garanties appropriées ont bien été prises lorsque la situation l'exige (voir la fiche n°10 « Les transferts de données hors Union européenne en cas de recours à des prestataires numériques ») ;
- suivre et identifier les destinataires de données à caractère personnel d'une personne donnée (nom et coordonnées électroniques au minimum), par exemple en configurant ses systèmes informatiques et logiciels de façon à retracer de manière fiable les destinataires de données à caractère personnel ;
- mener des analyses d'impact sur la protection des données (AIPD, ou études d'impact sur la vie privée) pour les traitements de données susceptibles d'engendrer un **risque élevé pour les droits et libertés des personnes physiques** (article 35 du RGPD). Les analyses d'impact permettent de satisfaire aux principes d'*accountability* et de *privacy by design* (cf. *supra*). L'obligation d'effectuer une analyse d'impact concerne les traitements répondant à au moins deux critères de la liste ci-après [24] :
  - 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,
  - et exclusion du bénéfice d'un droit/contrat.

24. Les 9 critères, issus de l'article 35 et de différents considérants du RGPD, sont récapitulés au sein des **lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) […].**

À ce titre, le traitement de gestion des dossiers des clients semble devoir par exemple faire l'objet d'une analyse d'impact (car au moins deux critères peuvent s'appliquer, comme la collecte de données sensibles [1] de personnes vulnérables [2]).

NOTA : la Cnil publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise, et parmi lesquelles figurent les traitements mis en œuvre par les avocats exerçant à titre individuel, cette exemption n'étant pas applicable aux structures d'exercice.

L'AIPD doit être réalisée avant la mise en œuvre effective de tout nouveau traitement de données qui en nécessiterait, par exemple en amont d'un projet.

Un logiciel gratuit et *open source* a été développé par la Cnil afin de faciliter la réalisation des analyses d'impact le cas échéant : **https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil**.

Pour en savoir plus concernant les analyses d'impact : **https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd**.

PARTIE II
MISE EN CONFORMITÉ DU CABINET

1. MÉTHODOLOGIE DE MISE EN CONFORMITÉ

De manière générale, la Commission nationale de l'informatique et des libertés (Cnil) a développé une méthodologie en quatre étapes afin de faciliter la mise en conformité des responsables de traitements. Ces étapes correspondent :

- au recensement des traitements (cartographie) ;
- à la vérification des données traitées ;
- au respect des droits des personnes sur leurs données ;
- à la maximisation de la sécurité des traitements.

1.1. La cartographie des traitements de données personnelles

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

La Cnil préconise en ce sens de se poser les questions suivantes :

- Qui ?
- Quoi ?
- Pourquoi ?
- Où ?
- 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 de l'avocat associé ou de l'avocat exerçant à titre individuel. Il convient ainsi d'identifier la personne au sein du cabinet d'avocats qui exerce un niveau de décision élevé quant à la façon de traiter les données personnelles.

NOTA : selon le niveau d'intégration ou d'indépendance des avocats au sein de la structure, le responsable de traitement peut aussi désigner le cabinet en tant que personne morale.

Il peut y avoir plusieurs niveaux ou types de traitement avec des responsables de traitement différents selon les cas, par exemple sur le choix des moyens informatiques ou la mise en place d'une procédure de gestion des conflits ou encore la politique de développement des pratiques spécialisées.

- **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. traitant les données du cabinet sur les instructions de ce dernier.

Quoi ? Il s'agit ici de savoir quels types de traitements sont effectués et quelles sont les données à caractère personnel que le cabinet collecte. En outre, il appartient à l'avocat d'identifier la présence de catégories particulières de données personnelles énoncées à l'article 9 du RGPD (données de santé, données concernant l'orientation et/ou la vie sexuelle, données concernant les orientations politique, philosophique et/ou religieuse, etc.) ou celles énoncées à l'article 10 du RGPD (données d'infraction et de condamnations pénales).

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, vigilance LCB-FT, etc.).

Où ? À 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'avocats ? etc.). Cette question doit également permettre à l'avocat d'identifier les éventuels transferts de données vers des pays hors Union européenne (un dossier international, un avocat postulant à l'étranger, etc.).

(Jusqu'à) Quand ? Le cabinet d'avocats a-t-il mis en place des durées de conservation pour les données à caractère personnel ? Le cabinet d'avocats a-t-il prévu une purge des données qu'il collecte ?

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

L'ensemble des éléments recensés doit être reporté et listé dans **le registre des traitements** (voir le point 3).

1.2. La vérification des données traitées

La cartographie des traitements dans leur ensemble permet de faire le tri dans les données traitées par l'avocat et de vérifier que les obligations en matière de protection des données sont bien respectées (voir le point 3 de la partie I).

Le cabinet d'avocats devra ainsi vérifier notamment :

- que les données traitées soient bien pertinentes et nécessaires à l'objectif poursuivi (principe de minimisation) ;
- la nature des données traitées afin de mettre en œuvre des mesures de sécurité adaptées aux risques spécifiques associés à ces données : l'avocat traite souvent dans le cadre de ses missions des catégories particulières de données (dites « sensibles ») ainsi que des données relatives aux condamnations pénales et aux infractions ou le numéro d'identification national auxquels il doit accorder la plus grande attention ;

- que les données soient traitées sur un fondement juridique défini par le RGPD (conclusion et exécution d'un contrat, nécessité de se conformer à une obligation légale, consentement, intérêt légitime du responsable de traitement, etc.) ;
- que seules les personnes habilitées aient accès aux données dont elles ont besoin ;
- que les données ne soient pas conservées au-delà de ce qui est nécessaire en fixant précisément la durée de conservation et d'archivage des données (principe de durée limitée de conservation des données) comme il en est question à la fiche n°2 (voir la partie III) ;

1.3. Le respect des droits des personnes

Les cabinets d'avocats doivent être extrêmement vigilants quant au respect de l'ensemble des droits que les personnes concernées ont sur leurs données personnelles. À ce titre, ils doivent :

- vérifier que leurs clients, fournisseurs, collaborateurs, salariés, etc. soient parfaitement informés du traitement des données : cette information doit être fournie au moment de la collecte, par exemple par le biais d'une page relative à la protection des données personnelles ou d'une notice d'information sur le site Internet du cabinet, de mentions écrites dans les conventions d'honoraires, contrats de collaborations, contrats de travail, etc ;
- respecter des procédures en interne pour mieux appréhender les demandes relatives aux différents droits des personnes : en effet, plus le cabinet d'avocats réagit rapidement en faisant droit aux demandes de droit d'accès, d'opposition, de rectification, etc., moins il ne prend le risque que les personnes portent plainte devant la Cnil ou devant les juridictions ;
- mettre en place des mesures internes relatives aux violations des données personnelles à savoir la notification à l'autorité de contrôle et la communication aux personnes concernées.

1.4. Renforcer la sécurité des données

Le cabinet d'avocats doit mettre en place un niveau adapté de mesures techniques et organisationnelles pour garantir la sécurité des données, et ce afin d'éviter trois types de risques : l'accès illégitime à des données, leur modification non désirée et leur disparition.

Afin de diminuer la probabilité que ces risques ne se matérialisent, le cabinet doit se poser les bonnes questions, et notamment :

- Les accès aux locaux sont-ils sécurisés ?
- Les armoires et coffre-fort sont-ils fermés à clés systématiquement ?
- Les comptes utilisateurs sont-ils protégés par des mots de passe d'une force suffisante ?
- Les postes de travail sont-ils sécurisés (ex : verrouillage automatique de session, antivirus, pare-feu, logiciels à jour, etc.) ?
- Les associés, collaborateurs et/ou personnels sont-ils sensibilisés à la protection des données et à la cybersécurité (et notamment aux attaques de type *phishing*[25] et « fraude au Président »[26]) ?

25. En français « hameçonnage », pratique frauduleuse consistant à induire un internaute en erreur et l'inciter à communiquer des informations personnelles (comptes d'accès, mots de passe, etc.) en se faisant passer pour un tiers de confiance (par exemple *via* un faux site Internet reprenant l'apparence du vrai).

26. Sur ce sujet, voir la **publication** de la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF).

- Une charte informatique a-t-elle été édifiée ? Le personnel est-il notamment empêché de télécharger des logiciels ou d'utiliser certains outils (notamment les intelligences artificielles) sans autorisation ?
- Des mobiles multifonctions (smartphones), ordinateurs portables, clés USB, disques durs amovibles ou tout équipement nomade sont-ils utilisés ? Leur usage est-il encadré ? Le personnel utilise-t-il ses propres appareils et, dans ce cas, une politique a-t-elle été mise en place pour encadrer strictement la séparation des données purement privées des données professionnelles, quitte à interdire complètement cette pratique ?
- Des procédures de sauvegardes régulières (certaines devant être effectuées « hors ligne ») et de récupération des données en cas d'incident ont-elles été mises en place ?
- La protection des données personnelles est-elle prise en compte dès le démarrage de tout nouveau projet et/ou avant l'adoption de tout nouvel outil numérique ? Le niveau de sécurité par défaut est-il toujours paramétré pour être le plus élevé ?
- Des habilitations strictes ont-elles été mises en place afin qu'une personne au sein du cabinet ne puisse pas accéder à une donnée qui ne la concerne pas ?

Pour en savoir plus concernant la sécurité et la confidentialité des données, il est renvoyé à la fiche n°6 « Les bonnes pratiques en termes de sécurité des données ».

2. RÔLES ET RÉPARTITION DES RESPONSABILITÉS

Dans le cadre de ses missions, l'avocat est amené à traiter des informations personnelles, notamment celles de ses clients et des personnes impliquées dans un dossier. En fonction des situations, l'avocat ne sera pas considéré de la même manière au regard du RGPD, notamment comme responsable de traitement ou, extrêmement rarement, comme sous-traitant.

Cette qualification est importante car elle détermine l'entité chargée de faire respecter les règles en matière de protection des données, la manière dont les personnes concernées peuvent exercer leurs droits dans la pratique et l'obligation de signer des clauses spécifiques en cas de sous-traitance RGPD (voir notamment le modèle de clauses en annexe).

2.1. L'avocat en tant que responsable de traitement

Le responsable de traitement est défini à l'article 4 point 7 du RGPD[27] comme étant « 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 ». Comme déjà énoncé au sein du guide, le responsable de traitement est celui qui a la maîtrise du pourquoi et du comment du traitement. Cette qualification se mesure finalement à l'aune de l'autonomie dans la mise en œuvre et la gestion d'un traitement de données personnelles.

27. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4

Une première situation concerne l'avocat dans la gestion des traitements de données « internes » à son cabinet (communication, ressources humaines, facturation, etc.). Ce cadre ne présente aucune difficulté, l'avocat est naturellement responsable de traitement. Une seconde situation concerne l'activité judiciaire de l'avocat vis-à-vis de ses clients. Le fait que celui-ci traite des données personnelles pour le compte de ses clients par mandat pourrait amener à penser qu'il est un sous-traitant au sens du RGPD. Néanmoins, cette possible ambiguïté est écartée par le caractère indépendant de l'avocat, confirmé par les avis et lignes directrices successifs du CEPD qui considère de longue date l'avocat comme responsable de traitement dans ce cadre :

> L'entreprise ABC mandate un cabinet d'avocats pour la représenter dans un litige. Pour mener à bien cette mission, le cabinet d'avocats doit traiter les données à caractère personnel relatives à l'affaire. Les raisons qui régissent le traitement des données à caractère personnel sont le mandat du cabinet d'avocats de représenter son client en justice. Ce mandat ne vise toutefois pas spécifiquement le traitement de données à caractère personnel. Le cabinet d'avocats agit avec un degré considérable d'indépendance, par exemple pour décider quelles informations doivent être utilisées et comment et l'entreprise cliente n'a pas donné d'instructions concernant le traitement des données à caractère personnel. Le traitement effectué par le cabinet d'avocats pour remplir sa mission de représentant légal de l'entreprise est donc lié au rôle fonctionnel du cabinet, de sorte que celui-ci doit être considéré comme étant le responsable de ce traitement.

Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD - V2 - Adoptées le 7 juillet 2021 [28]

Une troisième situation concerne les activités juridiques de prestation de conseil. Ici encore, la totale indépendance de l'avocat quant aux moyens utilisés fait de lui un responsable de traitement.

2.2. L'avocat en tant que sous-traitant

Le sous-traitant est défini à l'article 4 point 8 du RGPD comme étant « *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* ».

L'ancien guide de la Cnil « Les avocats et la loi Informatique et libertés » de 2011 évoquait le cas particulier des audits où les avocats pouvaient être considérés comme des sous-traitants au sens de la loi Informatique et libertés d'alors, arguant du fait qu'ils agissent « *sur la base d'instructions strictement définies par leurs clients* ».

Ainsi, s'il était établi que l'avocat exerçait une activité de collecte et compilation d'informations sur les strictes instructions et délimitations du client, sans aucune forme d'autonomie ou d'analyse juridique, il pourrait être considéré comme un sous-traitant. D'autres types de prestation pourraient être couverts par cette qualification, notamment si l'avocat réalise des missions délimitées pour le compte de ses clients comme une cartographie ou des tris de données, le renseignement de formulaires ou encore la simple réception d'alertes professionnelles à la demande du client.

28. https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_fr.pdf, page 14.

Néanmoins, l'indépendance de l'avocat fait que celui-ci ne doit pas être considéré comme un sous-traitant au sens du RGPD ni même comme un prestataire lambda. Ainsi, l'avocat ne devrait jamais faire signer de clauses le qualifiant de sous-traitant vis-à-vis de ses clients, étant entendu qu'une qualification ainsi retenue ne serait pas sans conséquence. Dans un même ordre d'idées, la réponse par un avocat à un marché public et sa qualité de titulaire s'il le remportait, s'il fait de lui un prestataire pour l'acheteur public, ne fait pas de lui un sous-traitant[29] (identique par analogie concernant un marché privé).

En tout état de cause, l'éventuelle reconnaissance de l'avocat comme sous-traitant dans le cadre d'un contrat, laissée à la libre appréciation du cabinet et en négociation avec un client, entraînerait la signature de clauses de sous-traitance conformément à l'article 28 du RGPD[30] (voir le modèle de clauses de sous-traitance en annexe).

2.3. Le cas particulier de la qualification de l'avocat collaborateur

La qualification du collaborateur est plus complexe car ce dernier, libéral ou salarié, peut traiter les dossiers du cabinet ou bien ses dossiers personnels. Le principe d'indépendance que doit respecter l'avocat dans l'exercice de la profession va avoir une incidence sur la qualification de l'avocat collaborateur dans ses relations avec le cabinet d'avocats avec lequel il travaille.

L'article 14 du Règlement intérieur national[31] rappelle « *l'indépendance qu'implique le serment d'avocat* », autant pour le collaborateur libéral que salarié sans lien de subordination avec le cabinet sinon pour ce qui concerne les conditions de travail.

En application de cette règle, l'avocat collaborateur ne semble pas pouvoir être assimilé à un sous-traitant du cabinet. Lorsque les collaborateurs/salariés traitent des données personnelles pour les besoins des dossiers du cabinet ou d'autres activités du cabinet, ce dernier est responsable de traitement et le collaborateur agit comme une personne autorisée à traiter ces données personnelles (articles 4.10, 29, 32.4 du RGPD).

Concernant l'avocat collaborateur qui utilise les moyens du cabinet pour le traitement de ses dossiers personnels, dans ce cadre strict, il est responsable de traitement et le cabinet, traitant des données pour le compte de ce premier, pourrait être considéré comme son sous-traitant, même si cela soulève d'innombrables problèmes pratiques quant au respect impossible de l'article 28 du RGPD. La difficulté naît de ce que la mise à disposition du collaborateur des moyens informatiques du cabinet ne résulte pas d'une prestation de service volontaire, mais d'une obligation déontologique.

Toutefois, si la gestion des dossiers personnels est opérée *via* des moyens informatiques mis en œuvre par des prestataires externes et que les logiciels et le système d'information n'ont pas été développés directement par et pour le cabinet, le cabinet ne sera pas considéré comme le sous-traitant du collaborateur libéral pour la gestion de ses dossiers personnels.

À FAIRE	
Identifier les différentes situations et les caractériser en fonction de la latitude laissée à l'avocat	☐

29. Cour administrative d'appel de Lyon, 4e ch., 18/06/2015, 14LY02786.
30. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article28
31. https://www.cnb.avocat.fr/fr/reglement-interieur-national-de-la-profession-davocat-rin.

3. LES PRINCIPAUX DOCUMENTS DE LA CONFORMITÉ

3.1. Le registre des activités de traitement

Le RGPD prévoit l'instauration d'un registre des activités de traitement, outil de documentation et de pilotage de la conformité, qui doit être tenu par l'avocat en tant que responsable de traitement ou exceptionnellement en tant que sous-traitant (voir le point 2).

Chaque responsable de traitement et sous-traitant doit tenir un registre des catégories de traitement de données à caractère personnel mises en œuvre sous sa responsabilité. Le RGPD énonce que cette obligation ne s'impose pas aux organismes comptant moins de 250 employés, sauf si le traitement qu'ils 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[32].

Il semble donc que les avocats, du simple fait que les traitements qu'ils mettent en œuvre sont pérennes et portent la plupart du temps sur des données relatives à des catégories particulières de données ou des données se rapportant à des condamnations et des infractions pénales, sont soumis à l'obligation de mettre en place un registre des activités de traitement comportant autant de fiches qu'il existe de traitements concernés par les exceptions susvisées.

En tout état de cause, la tenue d'un registre participe au respect du principe d'*accountability* (consistant à documenter la conformité pour pouvoir la prouver, voir le point 3.2 de la partie I).

Le registre, s'il ne fait l'objet d'aucun formalisme particulier (si ce n'est le fait d'être nécessairement écrit) doit, conformément à l'article 30.1 du RGPD[33], 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 à 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.

32. Article 30.5 du RGPD.
33. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article30

En tout état de cause, rien ne s'oppose à ce que le registre comporte encore davantage d'informations ; la Cnil recommande d'ailleurs de l'enrichir de mentions supplémentaires/complémentaires afin d'en faire un outil de pilotage de la conformité le plus efficace possible [34].

Sur cette base, il est renvoyé à l'annexe « Registre type des activités de traitement en tant que responsable de traitement » pour les avocats, qui expose les éléments minimums demandés par le RGPD ainsi que des thématiques complémentaires (de fait facultatives).

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.)	☐
Élaborer le registre des activités de traitement	☐

3.2. La documentation relative aux violations de données

L'article 33.5 du RGPD [35] énonce que le responsable de traitement, comme l'avocat, doit documenter toute violation de sa sécurité, documentation pouvant se matérialiser par l'édification d'un registre prévu à cet effet. Dans certains cas, ces violations devront être notifiées à la Cnil et certains éléments communiqués potentiellement aux personnes concernées (cf. *infra*).

Une 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.

Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles [36]. Le RGPD ne liste pas les informations devant obligatoirement être documentées avec la même précision que pour le registre des traitements (voir le point 3.1), mais l'article 33.5 précité énonce tout de même que doivent figurer les informations concernant la violation, en commençant par les causes, les faits et les données personnelles en jeu, ainsi que les conséquences de cette violation et surtout les mesures prises par le responsable du traitement pour y remédier.

34. https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement
35. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article33
36. Le formulaire de notification de la Cnil (cf. *infra*) les présente de la façon suivante :
- Perte de la confidentialité *[signifie que quelqu'un a eu accès à des informations alors qu'il n'aurait pas dû y avoir accès],*
- *Perte de l'intégrité [signifie que les informations ont été altérées ou déformées],*
- *Perte de la disponibilité [signifie que les informations ne peuvent être consultées par les personnes concernées].*

Comme pour le registre des traitements, la pratique veut que la documentation relative aux violations de données soit la plus explicite possible, de façon à comprendre le contexte d'une situation présentant un risque de sécurité, et il apparaît pertinent que cette documentation soit aussi calquée sur les éléments devant potentiellement être notifiés à la Cnil (voir le point 3.2 de la partie I) et certains potentiellement communiqués aux personnes concernées (bien que toutes les violations ne débouchent pas forcément sur une notification et une communication externes, cf. *infra*). Peuvent ainsi être documentés :

- les date et heure de début et de fin, le cas échéant, de l'incident de sécurité (souvent estimées), date et heure de prise en connaissance du risque par l'avocat (qui peuvent être bien plus tardives), circonstances de cette prise de connaissance ;
- les origine, nature (perte de la confidentialité, perte de la disponibilité, perte de l'intégrité des données personnelles) et description détaillée de la violation de données ;
- les formes des données, type de données (et notamment s'il s'agit de données dites « sensibles »), opérations de traitement, nombre approximatif et type de personnes concernées par l'incident (et notamment s'il s'agit de personnes dites « vulnérables » : personnes handicapées, patients, personnes âgées, mineurs, salariés, etc.) ;
- les effets et conséquences probables de la violation de sécurité pour les personnes concernées ;
- les mesures de sécurité mises en œuvre pour contrer et atténuer les effets de la violation en fonction de la situation (blocage d'un compte à distance, modification du mot de passe, géolocalisation du matériel perdu, accès aux traces informatiques laissées par les pirates, etc.) ;

Sur ce sujet, un modèle de registre des violations de données est dispensé en annexe.

3.2.1. Notification auprès de la Cnil

Hormis les cas où la violation n'est pas susceptible d'engendrer de risque pour les droits et libertés des personnes physiques (situation plutôt rare en pratique), il conviendra de la **notifier** à la Cnil dans les meilleurs délais et si possible **au plus tard dans les 72 heures** après en avoir pris connaissance (article 33 du RGPD).

L'avocat est conscient que, confronté à une telle situation, il doit notifier une violation de données faisant peser un risque sur les personnes concernées non pas seulement s'il obtient la preuve que le risque s'est bien concrétisé **mais simplement si ce risque est susceptible de se matérialiser.**

Exemple : l'avocat égare une clé USB contenant des dossiers relatifs à ses clients. Malgré un état de fait critique, le professionnel est persuadé qu'il y a finalement assez peu de chance dans sa situation que quelqu'un ne mette la main sur cette clé et ses dossiers. Néanmoins, le simple fait qu'un tiers puisse potentiellement trouver la clé et accéder aux données personnelles qui y sont stockées suffit pour que la violation de données soit caractérisée et ne doive faire l'objet, dans la situation, d'une notification (c'est pourquoi il est, en application de l'obligation de sécurisation des données personnelles, fortement déconseillé de stocker les informations des clients sur des lecteurs amovibles ouverts à tous sans mesures de sécurisation particulière).

La notification de violation de données 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 toutes conséquences négatives : ce qui implique que, à la suite d'un problème touchant des données personnelles, le professionnel doit ainsi réagir immédiatement après la découverte de l'incident, et si possible dès avant la notification, pour trouver des solutions et atténuer ou tenter de faire cesser, autant que possible, le risque engendré par la violation.

La notification de violation de données pourra être réalisée *via* un formulaire en ligne mis à disposition sur le site Internet de la Cnil, transmettant directement par ce biais les éléments relatifs à une notification à l'autorité nationale de contrôle : **https://notifications.cnil.fr/notifications/index**.

Si l'incident de sécurité concerne un traitement opéré par un sous-traitant, celui-ci devra informer le cabinet de la violation dans les meilleurs délais après en avoir pris connaissance (en général pas plus de 48 heures), de façon à ce que ce dernier puisse effectuer en cas de risque pour les personnes concernées la notification à la Cnil. Cette notification pourra aussi être effectuée directement par le sous-traitant pour le compte du cabinet, il est recommandé dans ce cadre de le préciser contractuellement (voir l'annexe « Modèle de clauses de sous-traitance RGPD »).

3.2.2. Notification (communication) auprès des personnes concernées

Il conviendra également, si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, d'informer directement « dans les meilleurs délais » la personne concernée de la violation (article 34 du RGPD[37]). 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 » ;
- elle exigerait des efforts disproportionnés, le RGPD autorisant alors à la place une communication publique ou toute autre mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

La notion de « risque élevé » est précisée par les considérants 75 et 76 du texte européen et doit amener l'avocat à prendre en compte les paramètres suivants :

- le type de violation (affectant l'intégrité, la confidentialité ou la disponibilité des données) ;
- la nature, la sensibilité et le volume de données personnelles concernées ;
- la facilité d'identifier les personnes touchées par la violation ;
- les conséquences possibles de la violation et leur niveau de gravité pour ces personnes ;
- les caractéristiques de ces personnes (mineurs, personnes vulnérables, salariés, etc.) ;
- le volume de personnes concernées ;
- les caractéristiques du responsable du traitement (nature, rôle, activités).

37. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article34

NOTA : une violation touchant aux dossiers de l'avocat, notamment de par leur nature sensible et des conséquences probables négatives pour les clients et les autres personnes concernées, entrainera souvent un risque élevé pour les personnes concernées, nécessitant ainsi une information de ces personnes (sauf si l'une des exceptions à cette obligation ne s'applique, par exemple si les mesures techniques et organisationnelles ont rendu les données incompréhensibles pour toute personne). Cependant, il faudra évaluer avec grande précaution à qui la notification peut être faite et ce qu'elle peut contenir sans constituer un manquement au secret professionnel.

L'avocat, dans le cadre de cette communication de la violation aux personnes concernées, devra ainsi informer ces dernières :

- des nom et coordonnées du délégué à la protection des données ou d'un autre point de contact « RGPD » auprès du cabinet ;
- des conséquences probables de la violation de données à caractère personnel ;
- des mesures prises ou à venir pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les conséquences négatives.

Attention : si le cabinet d'avocats ne procédait pas à cette communication à la ou les personne(s) concernée(s) alors même qu'il y serait obligé, l'autorité de contrôle pourra, après avoir examiné le risque résultant de cette violation, enjoindre le responsable de traitement de procéder à cette communication. Le cas échéant, l'intervention du bâtonnier pourrait être envisagée.

À FAIRE	
Mobiliser les personnes compétentes au sein du cabinet	☐
Qualifier la violation de données	☐
Prendre les mesures nécessaires en vue d'atténuer les éventuelles conséquences	☐
Si **risque** pour les droits et libertés des personnes : notification à la Cnil	☐
Si risque **élevé** : communication auprès des personnes concernées après évaluation des autres obligations de l'avocat en matière de secret professionnel	☐
En tout état de cause, et quel que soit le niveau de risque, documenter l'incident et insérer son descriptif au sein d'un registre des violations de données pour plus de commodités	☐

4. LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Le délégué à la protection des données (DPD), ou *Data protection officer* (DPO) en anglais, est une nouvelle fonction créée par le RGPD. Il est chargé d'aider les responsables de traitement à mettre en conformité leurs traitements de données.

Le délégué à la protection des données doit être indépendant et ne doit pas recevoir d'instructions dans l'exercice de ses missions (article 38.3 du RGPD[38]). En ce sens, il ne devrait dépendre directement que du responsable de traitement (par exemple un avocat associé) et non d'un responsable fonctionnel. Cette indépendance est complétée par le fait que le DPD ne peut être ni relevé de ses fonctions ni pénalisé par le responsable de traitement.

NOTA : cette protection n'est toutefois pas absolue, le délégué n'étant pas d'ailleurs en France considéré comme un « salarié protégé », et ne peut empêcher son licenciement pour manquement aux règles internes d'un organisme, communes à tous les salariés (pour des motifs autres que l'exercice de ses missions), pas plus que dans une situation où le délégué ne possèderait plus les qualités professionnelles requises pour exercer ses missions ou ne s'acquitterait pas de celles-ci[39].

Enfin, le délégué est soumis au secret professionnel ou à une obligation de confidentialité (article 38.5 du RGPD).

Aux termes de l'article 37 du RGPD[40], 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.

NOTA : la désignation d'un délégué à la protection des données n'est donc pas conditionnée à un seuil en termes d'effectifs au sein d'un cabinet.

Pour la majorité des cabinets d'avocats, il ne semble pas qu'une telle désignation soit obligatoire dans la mesure où, s'ils traitent des catégories particulières de données ou des données relatives aux infractions et condamnations, les cabinets ne le font pas « à grande échelle » (cf. point suivant).

La Cnil a publié un **guide** spécifiquement consacré au délégué à la protection des données.

38. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article38
39. CJUE, 22 juin 2022, C-534/20.
40. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article37

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

Le CEPD a publié très tôt des lignes directrices[41] sur le rôle des délégués à la protection des données et a fourni des recommandations concernant les bonnes pratiques.

Les responsables de traitement peuvent opter pour un délégué à la protection des données en interne (salarié) ou en externe (prestataire de services), mutualisé ou non. Lorsqu'un délégué à la protection des données est nommé, le cabinet est tenu de procéder à sa désignation sur le site Internet de la Cnil : **https://designations.cnil.fr/dpo/designation/organisme.designant.delegue.action**.

Néanmoins, il est rappelé que la désignation du délégué à la protection des données est obligatoire 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, étant donné qu'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[42].
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, et à défaut, il est toujours opportun de nommer une personne en interne qui pourrait se charger des aspects liés à la protection des données et qui servirait de référent pour le personnel et les collaborateurs du cabinet.

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

Le RGPD impose des obligations importantes aux délégués à la protection des données. Véritable « 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 :

41. Lignes directrices concernant les délégués à la protection des données (DPD).
42. Sur ce sujet, voir la réponse de la Cnil : **https://www.cnil.fr/fr/cnil-direct/question/reglement-europeen-un-traitement-grande-echelle-cest-quoi.**

- 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 ;
- d'être le point de contact des personnes concernées.

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

4.3. Avocat agissant en tant que délégué à la protection des données

Opportunément, le RGPD a abrogé le seuil des 50 salariés qui interdisait d'externaliser l'ancien correspondant informatique et libertés (CIL), précurseur du délégué à la protection des données (DPO).

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)[43] de la profession d'avocat, adoptée par l'assemblée générale du Conseil national des barreaux des 9 et 10 décembre 2016[44] 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-DPO.

L'article 6.3.3 « Délégué à la protection des données » du RIN prévoit que : *« 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-DPO était déjà soumis à deux devoirs qui ne s'imposent pas au DPO non avocat : le devoir de non-dénonciation de son client et le devoir de démission en cas de conflit d'intérêts.

Il est ainsi apparu nécessaire de préciser que l'avocat doit refuser de représenter les clients pour lesquels il exerce ou a exercé la mission de DPO 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.

43. https://www.cnb.avocat.fr/reglement-interieur-national-de-la-profession-davocat-rin.
44. Publiée au *Journal officiel* du 13 avril 2017.

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

« 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 délégué à la protection des données doit en faire la déclaration à l'Ordre, par lettre ou courriel adressée au Bâtonnier. »

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 exercer ces missions, et d'autre part à permettre aux Ordres de communiquer sur les avocats exerçant ces missions dans leur ressort.

PARTIE III
BOÎTE À OUTILS (FICHES PRATIQUES)

Pour renforcer la conformité des traitements de données à caractère personnel et protéger au mieux ces dernières, plusieurs fiches pratiques sont proposées à l'attention des avocats et réparties suivant plusieurs thématiques :

- **La conformité des traitements de données du cabinet :**
  - **Fiche n°1 :** la gestion des clients
  - **Fiche n°2 :** la gestion des archives
  - **Fiche n°3 :** la gestion des ressources humaines
  - **Fiche n°4 :** la gestion des fournisseurs et prestataires
  - **Fiche n°5 :** la gestion de la lutte contre le blanchiment et le financement du terrorisme
- **La sécurisation des traitements de données du cabinet :**
  - **Fiche n°6 :** les bonnes pratiques en termes de sécurité des données
  - **Fiche n°7 :** la gestion de la vidéosurveillance/vidéoprotection
  - **Fiche n°8 :** la gestion des accès physiques
- **La numérisation des activités du cabinet :**
  - **Fiche n°9 :** la mise en conformité du site Internet
  - **Fiche n°10 :** les transferts de données hors Union européenne en cas de recours à des prestataires numériques
- **Les droits des personnes concernées par les traitements :**
  - **Fiche n°11 :** la gestion du droit d'accès aux données des personnes concernées
  - **Fiche n°12 :** les pouvoirs de contrôle de la Cnil

FICHE N° 1
LA GESTION DES CLIENTS

1. QUELLES DONNÉES L'AVOCAT PEUT-IL COLLECTER DANS LE CADRE DE LA GESTION DES DOSSIERS 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 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 très variées peuvent concerner des informations relatives tant à la vie personnelle qu'à la vie professionnelle mais également des données d'une particulière sensibilité.

Données relatives aux condamnations pénales et aux infractions. Le caractère particulier de ces données que l'avocat peut être amené à collecter 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 [45].

Toutefois, l'article 46 de la loi Informatique et libertés [46] prévoit que le traitement des données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes peut être effectué par les **auxiliaires de justice pour les stricts besoins de l'exercice des missions que la loi leur confie.**

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

Or, l'article 9, alinéa 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.

Cependant, l'article 9 prévoit notamment 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 ». Les avocats sont ainsi protégés par cette exception qui leur permet de traiter ces données particulières dans le cadre de l'exercice de leur profession.

45. Article 10 du RGPD.
46. https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006528180.

Respect du principe de minimisation. Ceci semble d'autant plus important que, conformément à l'article 5 du RGPD[47], 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 PRÉALABLES À LA MISE EN ŒUVRE DU TRAITEMENT ?

Le RGPD a supprimé la quasi-totalité des formalités préalables existantes et a introduit en contrepartie de nouvelles obligations pour le responsable de traitement comme la tenue d'un **registre des activités de traitement** dans lequel il convient d'insérer notamment une fiche dédiée à la gestion des dossiers des clients (voir l'annexe « Registre type des activités de traitement en tant que responsable de traitement »).

Également, une analyse d'impact sur la vie privée peut-être menée concernant ce traitement, plusieurs critères (voir le point 3.2 de la partie I) étant susceptibles d'être remplis :

- personnes vulnérables (potentiellement), par exemple des clients en grande difficulté ou précarité, des mineurs, des personnes handicapées, etc. ;
- données sensibles ou hautement personnelles (potentiellement), par exemple des informations médicales, relatives à l'orientation religieuse, sexuelle ou politique, des données relatives aux condamnations pénales et aux infractions, des informations relatives à la vie familiale, à la situation financière et au patrimoine, etc.

NOTA : les avocats exerçant à titre individuel sont exemptés de mener une analyse d'impact pour le traitement mis en œuvre dans le cadre de l'exercice de leur profession (cette exemption n'étant pas applicable aux structures d'exercice).

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.

47. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article5

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 (cinq ans) et pourraient même être conservées plus longtemps (voir la fiche n°2 « La gestion des archives »), étant cependant précisé que les actions disciplinaires ne sont pas limitées dans le temps.

4. DOIT-IL Y AVOIR UNE INFORMATION DES PERSONNES CONCERNÉES ?

Conformément aux exigences de l'article 13 du RGPD (voir le point 3.1.5.1 de la partie I), les clients et prospects du cabinet d'avocats doivent être informés des modalités de traitement de leurs données (finalité, destinataire des données, durée de conservation, etc.).

NOTA : le RGPD n'exige pas que l'information soit fournie par écrit, mais l'écrit fournit aux responsables de traitement la preuve du fait que l'information a été effectuée correctement.

5. LA SÉCURITÉ DES DOSSIERS CLIENTS

Comme évoqué au point 3.1.4 de la partie I, il est nécessaire de prendre des mesures de sécurité adaptées à la sensibilité des traitements (voir également la fiche n°6 « Les bonnes pratiques en termes de sécurité des données ») ; au-delà de cette exigence portée par le RGPD, l'avocat est soumis au secret professionnel absolu et se doit pour cette raison d'assurer la confidentialité des données qui lui sont confiées par ses clients.

Concrètement, tout comme pour les données RH (voir la fiche n°3 « La gestion des ressources humaines »), la sécurité des dossiers clients doit être l'une des priorités pour l'avocat en raison du caractère généralement sensible des données inscrites dans les dossiers.

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

L'avocat doit vérifier que les prestataires informatiques auxquels il fait appel pour héberger et traiter ses données présentent toutes les garanties suffisantes de sécurité. Si ces prestataires opèrent des transferts de données en dehors de l'Union européenne, ils peuvent avoir à mettre en œuvre des mesures supplémentaires de protection (voir la fiche n°10 « Les transferts de données en dehors de l'Union européenne en cas de recours à des prestataires numériques »).

L'avocat doit aussi s'assurer que les bases de données (y compris par exemple celle de la carte mémoire de l'imprimante) sont régulièrement effacées tout comme les documents papiers en fonction des durées de conservation.

Les cabinets doivent enfin organiser des formations sur la protection des données à caractère personnel et la cybersécurité auprès de ses membres et mettre en place un certain nombre de politiques internes (notamment une charte informatique et une procédure de gestion des violations de données).

6. SOLLICITATION PERSONNALISÉE

Au-delà du respect des exigences précitées, il existe des règles particulières applicables en matière de sollicitation personnalisée par voie électronique, téléphonique ou par voie postale.
À cet égard, un vade-mecum de la communication des avocats est disponible sur le site Internet du Conseil national des barreaux.

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	☐
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° 2
LA GESTION DES ARCHIVES

1. LES DONNÉES PERSONNELLES PEUVENT-ELLES ÊTRE CONSERVÉES *AD VITAM AETERNAM* ?

Les données personnelles ne peuvent pas être conservées de manière illimitée ; par défaut, les informations seront susceptibles d'être supprimées au-delà de l'utilisation courante du traitement, qui correspond à la durée nécessaire à la réalisation de l'objectif du traitement, s'il n'y a pas de raison de les conserver (voir le point 3.1.3 de la partie I).

Toutefois, cette obligation de fixer une durée de conservation limitée dans le temps ne prive pas les avocats de la possibilité d'archiver les informations, notamment à des fins probatoires, et de les conserver ainsi plus longtemps même si elles ne leur sont plus utiles directement.

Ainsi, au terme de la réalisation de la finalité du traitement, les données doivent :

- être effacées, ou
- être archivées (cf. *infra*), ou
- faire l'objet d'un processus d'anonymisation des données, afin de rendre impossible la « réidentification » des personnes. Ces données, n'étant plus à caractère personnel, peuvent dans ce cadre être conservées librement et valorisées notamment pour la production de statistiques.

Attention : en cas de procédure de suppression automatique, le responsable du fichier doit s'assurer que les données sont effectivement supprimées.

Les données à caractère personnel peuvent aussi être conservées au-delà de la durée maximum dans la mesure où elles sont traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le choix des données conservées à des fins archivistiques dans l'intérêt public est opéré dans les conditions prévues à l'article L. 212-3 du Code du patrimoine[48] (considérants 39 et 45 et article 5, 1°, e) du RGPD et article 4 de la LIL.

Concernant le cycle de vie de la donnée, la Cnil préconise trois phases :

- 1) la base active,
- 2) l'archivage intermédiaire,
- 3) l'archivage définitif.

48. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037825470

1re phase : la base active

C'est la durée d'utilisation courante des données, autrement dit la durée nécessaire à la réalisation de la finalité du traitement.

2e phase : l'archivage intermédiaire

Il peut être justifié que les données personnelles soient conservées pour des durées plus longues en archivage intermédiaire distinctement de la base active (le dossier étant considéré comme « clos »), avec accès restreint, dans la mesure où :

- il existe une obligation légale de conservation de données pendant une durée fixée ;
- en l'absence d'obligation de conservation, ces données présentent néanmoins un intérêt administratif, notamment en cas de contentieux, justifiant de les conserver le temps des règles de prescription/forclusion applicables, notamment en matière commerciale, civile et fiscale ;
- enfin, sous réserve de garanties appropriées pour les droits et libertés des personnes concernées, certaines données peuvent être traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques (cf. *supra*).

Néanmoins, l'archivage n'est pas systématique et les durées de conservation fixées dans ce cadre nécessiteront d'être justifiées ; ainsi, il appartiendra à l'avocat responsable de traitement de documenter l'analyse justifiant la mise en place d'un archivage intermédiaire et la durée retenue pour cet archivage.

Également, la conservation de la donnée doit respecter un certain schéma afin de garantir la sécurité de ces données. Ainsi, les archives, physiques comme numériques, doivent être dissociées de la base active et cloisonnées de sorte que seules des personnes dûment habilitées puissent y accéder et uniquement en cas de motif légitime (séparation logique).
Lorsque cet archivage est réalisé sous forme électronique, il convient de respecter la recommandation de la Cnil [49] sur la question.

3e phase : l'archivage définitif

Cette dernière phase concerne des données archivées sans limitation de durée, uniquement pour les traitements mis en œuvre à des fins archivistiques dans l'intérêt public. L'accès aux données ainsi archivées est très limité.

Cela peut concerner l'action disciplinaire qui est imprescriptible (Conseil constitutionnel, décision n°2018-738 du 11 octobre 2018 [50]).

49. Délibération 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel.
50. https://www.conseil-constitutionnel.fr/decision/2018/2018738QPC.htm.

2. COMMENT DÉFINIR LA DURÉE DE CONSERVATION D'UNE DONNÉE ?

La durée de conservation est fixée par le responsable de traitement et elle sera le fruit de la combinaison de plusieurs paramètres. Elle dépendra de la nature des données, des objectifs poursuivis et du principe de prudence.

En effet, si un texte impose une durée précise, il faudra bien évidemment le respecter.

En l'absence d'obligation de conservation clairement définie, à l'issue de la période d'utilisation courante des données personnelles, l'avocat responsable de traitement peut conserver les données plus longtemps si ceci présente un intérêt juridique (tel que se prémunir d'un contentieux spécifique), le temps des règles de prescription/forclusion applicables, notamment en matière commerciale, civile et fiscale.

Pour dégager une ligne directrice concernant l'archivage opérationnel, intermédiaire et définitif du cabinet, il faut garder à l'esprit qu'un cabinet possède une diversité de métiers qui font sa richesse, mais également sa complexité.
En effet :

- **en matière comptable, le délai légal de conservation est de 10 ans** à partir de la clôture de l'exercice en application de l'article L. 123-22 du Code de commerce[51] ;
- **en matière fiscale, le délai légal de conservation est de six ans** à compter de la dernière opération mentionnée sur les livres ou registres ou de la date à laquelle les documents ou pièces ont été établis en application de l'article L. 102 B du Livre des procédures fiscales[52] ;
- **en matière de gestion du personnel** (bulletin de paie, RUP, document concernant les contrats de travail, salaires, primes, indemnités, soldes de tout compte, régimes de retraite, etc.), **plusieurs délais se combinent et fixent le délai à cinq ans** après le départ du salarié de l'entreprise (retraite ou autre), ce qui est le délai minimum. En matière pénale, la prescription pour les cas de harcèlement moral, sexuel, téléphonique est de six ans ;
- en **matière d'action mobilière,** le délai de prescription est de cinq ans à compter du jour où le titulaire d'un droit a connu ou aurait dû connaître les faits lui permettant de l'exercer (article 2224 du Code civil[53]).

Dans le cas d'un dossier clôturé, le cabinet pourra ainsi rendre les originaux après en avoir fait une copie, à moins que la détention de ces documents ne soit requise par les textes, et ne conserver que les données pertinentes en cas de contentieux et archiver le dossier pendant cinq ans, au-delà de quoi le dossier pourra être détruit s'il n'y a pas eu de réclamation.

Par ailleurs, l'article 2232 du Code civil[54] dispose que *« le report du point de départ, la suspension ou l'interruption de la prescription ne peut avoir pour effet de porter le délai de la prescription extinctive au-delà de vingt ans à compter du jour de la naissance du droit ».*

51. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006219327
52. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000041471233
53. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000019017112
54. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033033506

En conséquence, le délai de conservation des documents pourrait être porté à un minimum de 10 ans voire de 20 ans par application de l'article précité.

Il faudra donc opérer un arbitrage entre la prudence et les impératifs légaux ou réglementaires d'un côté et la gestion d'une politique d'archivage raisonnée de l'autre (ce qui sera conservé et à partir de quand les données pourront être détruites). Il est rappelé que les sanctions disciplinaires des avocats ne sont pas prescriptibles.

3. COMMENT SÉCURISER LES ARCHIVES DE MANIÈRE OPTIMALE ?

Il convient fondamentalement de sécuriser les archives afin de les mettre à l'abri de toutes intrusions ou/et divulgations.
La sécurisation des archives est primordiale et pourra notamment s'opérer grâce à la numérisation, permettant dans un même temps de réduire considérablement le métrage linéaire d'archives.
Cependant, lorsque sont opérées une dématérialisation et une numérisation des documents, il convient de veiller à respecter les normes d'archivage afin d'accorder une force probante aux documents numérisés par rapport aux originaux.

Il est rappelé que le passage de la « base active » (relation contractuelle) à « l'archivage intermédiaire » (conservation du dossier clos en cas de contentieux), après un premier tri des informations personnelles, sera marqué par :

- l'extraction des données pour les conserver séparément dans une base d'archivage dédiée (papier ou numérique) à laquelle seules quelques personnes spécifiquement habilitées pourront accéder (séparation physique) ;
- ou la conservation des dossiers clos au même endroit que les dossiers en cours mais avec une identification claire et des mesures de sécurité prises pour rendre ces premiers inaccessibles aux personnes n'ayant plus d'intérêt à les traiter (par exemple, les avocats collaborateurs ayant travaillé sur le dossier ne devraient plus bénéficier des droits pour accéder aux données, seuls les avocats associés seraient habilités à y accéder pour des utilisations ponctuelles et exceptionnelles, sans possibilité de modifier les données et avec une traçabilité de leurs accès).

Une autre méthode d'archivage sécurisé est la pseudonymisation des documents avec un chiffrement des données, l'avocat responsable de traitement étant seul en possession d'une clé de déchiffrage.

NOTA : les données pseudonymisées diffèrent des données anonymisées (ne pouvant plus être reliées à un individu) et, à ce titre, rentrent toujours dans le champ du RGPD.

Enfin, la consultation des données archivées doit être tracée. Une personne exerçant par exemple son droit d'accès doit obtenir la communication des données qui la concerne, sous réserve du respect du secret professionnel, qu'elles soient stockées en base active ou archivées, et l'accès aux données par les avocats ayant répondu à cette demande doit être consigné dans un registre ou tout document prévu à cet effet.

4. LES BONNES QUESTIONS À SE POSER EN TERMES DE CONSERVATION ET D'ARCHIVAGE DES DONNÉES

- Jusqu'à quand ai-je vraiment besoin des données pour atteindre l'objectif fixé ?
- Ai-je une obligation légale de conserver les données pendant un certain temps ?
- Dois-je conserver certaines données en vue de me protéger contre un éventuel contentieux ? Si oui, lesquelles ?
- Jusqu'à quand puis-je faire valoir ce recours en justice ?
- Quelles informations doivent-elles être archivées ? Pendant combien de temps ?
- Quelles sont les règles de suppression des données ?
- Quelles sont les règles d'archivage des données ?

À FAIRE	
Vérifier que des durées de conservation ont été définies pour les données traitées par le cabinet	☐
Vérifier que les durées ne sont pas définies par des textes	☐
Vérifier que les durées ne sont pas définies par des recommandations de la Cnil ou des règles professionnelles	☐
Appliquer des durées d'archivage correspondant aux délais de prescription/forclusion applicables	☐
Définir une politique de durée de conservation	☐
Prendre connaissance du référentiel des durées de conservation en annexe et l'enrichir/ le mettre à jour	☐
Vérifier que les dossiers archivés sont correctement protégés et sécurisés	☐

FICHE N° 3
LA GESTION DES RESSOURCES HUMAINES

1. QU'EST-CE QU'UN TRAITEMENT RH ?

Dans le cadre du recrutement d'un avocat collaborateur ou 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 en conformité avec le RGPD.

La Cnil a publié en ce sens un **référentiel** spécifiquement consacré aux traitements de données relatifs à la gestion des ressources humaines mais qui traite davantage des relations salariées que les relations dans le domaine des professions libérales.

2. QUELLES SONT LES DONNÉES QUE L'AVOCAT PEUT COLLECTER DANS LE CADRE D'UN TRAITEMENT RH ?

De manière générale, 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 en respect du principe de minimisation (voir le point 3.1.2 de la partie I).

Recrutement. Dans le cadre du recrutement, les données ne doivent servir qu'à évaluer les aptitudes et compétences professionnelles du candidat et la capacité de ce dernier à occuper l'emploi proposé (article L. 1221-6 du Code du travail [55]).

Ainsi, seules des données relatives à la qualification et à l'expérience du collaborateur peuvent être collectées (formation, diplômes, fonctions précédemment occupées, etc.).

Il est donc interdit, par exemple, de :

- collecter des données sur la famille du candidat ;
- collecter des données sur les opinions politiques ou l'appartenance syndicale du candidat ;
- collecter des données sur le statut amoureux ou marital du candidat ou encore sur le fait de savoir si la personne est enceinte ou compte avoir un enfant dans un avenir proche ;

55. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006900845

- demander à un candidat la communication de son numéro de Sécurité sociale (ceci ne peut être fait que pour un candidat retenu ET ayant accepté la proposition d'embauche), etc.

La Cnil a publié un **guide** dédié à la gestion des données personnelles dans le cadre du recrutement.

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 et traiter principalement deux types de données :

- Des données nécessaires au respect d'une obligation légale (par exemple la transmission sur demande à l'administration fiscale du montant des rémunérations de leurs salariés) étant précisé que les obligations sont différentes en ce qui concerne les salariés et les collaborateurs profession libérale ou encore les associés.
- Des données utiles à la (i) gestion administrative du personnel, (ii) à l'organisation du travail et (iii) à l'action sociale, de manière générale.

Contrôle ou restrictions concernant l'utilisation des outils de travail. L'avocat employeur peut mettre en place différents outils afin de maîtriser l'activité des collaborateurs et/ou du personnel, ou du moins d'empêcher certaines actions présentant un danger pour la sécurité et la confidentialité des données.

Par exemple, le cabinet d'avocats pourrait encadrer les conditions d'utilisation d'Internet sur le lieu de travail. Il peut mettre en place des filtres afin de bloquer certains contenus (pornographie, pédophilie, etc.). Il est également possible, ceci rejoignant les mesures de sécurité, de limiter l'utilisation d'Internet pour des raisons de sécurité en empêchant notamment l'installation voire le téléchargement de logiciels non autorisés, l'inscription à un forum, le téléchargement de pièces jointes *via* le Webmail, ou d'utiliser les outils d'intelligence artificielle d'une façon qui mette en danger la confidentialité des données, etc.

En ce qui concerne le contrôle de l'activité, le respect de la vie privée résiduelle sur les temps et lieu de travail doit néanmoins être pris en compte avant la mise en œuvre de telles mesures.

Contrôle du temps passé. Un cabinet peut mettre en place un système permettant aux personnes intervenant sur un dossier d'enregistrer le temps passé sur un dossier ou une affaire pour les besoins de facturation au temps passé ou de budgétisation, voire de l'attribution de bonus ou de primes.

Gestion et contrôle de l'accès au cabinet d'avocats. Un cabinet d'avocats peut mettre en place des dispositifs afin de contrôler l'accès du personnel (voir la fiche n°8 « La gestion des accès physiques »).

Attention : il est obligatoire pour les cabinets d'avocats, en tant que responsables de traitement, d'informer leurs salariés de tout dispositif de contrôle par note de service ainsi que le Comité social et économique (CSE) pour avis le cas échéant (cabinet de plus de 11 salariés), et plus généralement de tous les types de traitement de données à caractère personnel concernant les personnels du cabinet.

3. L'AVOCAT DOIT-IL PROCÉDER À DES FORMALITÉS PRÉALABLES EN CAS DE TRAITEMENT RH ?

Le RGPD a supprimé la quasi-totalité des formalités préalables existantes et a introduit en contrepartie de nouvelles obligations pour le responsable de traitement[56] comme la tenue d'un **registre des activités de traitement** dans lequel il convient d'insérer notamment des fiches dédiées à la gestion des ressources humaines en fonction des différentes finalités (recrutement, formation, paie, vidéosurveillance, etc.) dont vous trouverez des modèles en annexes.

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.

Exemples de durées de conservation appliquées à des traitements RH :

TRAITEMENTS DE DONNÉES	DURÉES DE CONSERVATION
Recrutement (CV, lettre de motivation, etc.)	2 ans au maximum en base active*
Paie	5 ans au minimum**
Dossier du salarié	5 ans après le départ du salarié
Contrôle des accès	3 mois
Vidéosurveillance	30 jours (grand maximum)

* L'avocat employeur peut conserver, par exemple 3 mois après la fin du recrutement, les documents des candidats non retenus afin d'être en mesure de leur apporter des explications sur les raisons ayant conduit au rejet de leur candidature. L'employeur peut ensuite souhaiter conserver, pour une durée raisonnable qui ne devrait pas dépasser deux ans, les informations relatives à un candidat qui n'a pas été retenu afin de pouvoir le recontacter ultérieurement en cas de nouvelles opportunités d'emploi (nouveau traitement de « vivier de candidatures » pour lequel le consentement du candidat à la conservation de son dossier est requis). Enfin, l'avocat peut également conserver les informations relatives à un candidat à des fins probatoires afin de se prémunir notamment contre d'éventuelles actions pour discriminations (voir la fiche n°2 « La gestion des archives » ainsi que le modèle de référentiel des durées de conservation en annexe.).

** Concernant les bulletins de paie dématérialisés, l'avocat employeur doit les garder disponibles pour ses salariés et ex-salariés en archives pendant 50 ans ou jusqu'à ce que le salarié atteigne l'âge théorique de 75 ans.

56. Les cabinets d'avocats auront généralement en matière de ressources humaines la qualité de responsable de traitement (RT), mais, dans certains cas aussi, celle de co-RT (avec par exemple un cabinet de recrutement qui participerait à la phase de recrutement *via* un service que ce dernier mettrait à la disposition des avocats constitué d'une base de données intégrant à la fois les CV reçus par le cabinet d'avocats et ceux déjà présents dans la base).

5. DOIT-IL Y AVOIR UNE INFORMATION DES PERSONNES CONCERNÉES ?

Conformément aux exigences de l'article 13 du RGPD (voir le point 3.1.5.1 de la partie I), les collaborateurs et le personnel du cabinet d'avocats doivent être informés des modalités de traitement de leurs données (finalité, destinataire des données, durée de conservation, etc.) étant précisé qu'il y aura nécessairement des différences entre le traitement des données des salariés, des collaborateurs profession libérale et des associés.

L'information devant être fournie au moment où les données sont obtenues, les membres du cabinet ont déjà été informés du traitement de leurs données transmises dans le cadre de leur recrutement, et le sont à nouveau par exemple *via* le contrat de collaboration ou de travail pour les nouvelles données communiquées et aux fins des nouveaux traitements découlant de la signature de ce contrat.
Les informations peuvent également faire l'objet d'un affichage physique au sein du cabinet ou d'une communication par courriel.

NOTA : le RGPD n'exige pas que l'information soit fournie par écrit, mais l'écrit fournit aux responsables de traitement la preuve du fait que l'information a été effectuée correctement.

6. QUEL EST LE NIVEAU DE SÉCURITÉ ADÉQUAT POUR LES DONNÉES RH ?

Si les informations personnelles des clients sont généralement d'une grande sensibilité (données hautement personnelles, sensibles et/ou relatives aux infractions et condamnations pénales), les données RH du personnel et des collaborateurs des cabinets le sont tout autant.

En effet, si l'on prend la définition et la liste des « catégories particulières de données » (données de santé, données relatives à l'orientation sexuelle, politique, religieuse, etc.) énoncées par le RGPD (article 9), plus communément appelées « données sensibles », ainsi que les données d'infraction et de condamnations pénales (article 10), bon nombre de documents et pièces RH rentrent pleinement dans cette acceptation, et notamment :

- la reconnaissance de la qualité de travailleur handicapé (RQTH) ;
- l'appartenance syndicale des personnes lors d'éventuelles élections professionnelles ;
- les arrêts maladie, même si l'employeur n'a pas accès aux détails des deux premiers volets (l'arrêt pour raison médicale est en soi une information concernant la santé) ;
- l'extrait de casier judiciaire B3, etc.

En outre, le numéro de Sécurité sociale (NIR), utilisé en matière de ressources humaines (pour les payes des salariés notamment), bénéficie d'une protection particulière et ne peut être collecté et traité que dans des conditions strictement définies par les textes. Ainsi, l'utilisation du NIR est strictement limitée à ce qui est prévu dans le décret n°2019-341 du 19 avril 2019 relatif à la mise en œuvre de traitements comportant l'usage du numéro d'inscription au répertoire national d'identification des personnes physiques ou nécessitant la consultation de ce répertoire[57].

57. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038396526

Ainsi, la protection de ce type de données personnelles doit être aussi élevée que pour les autres données des clients traitées par le cabinet ou par un avocat exerçant à titre individuel, et ce afin de satisfaire à l'obligation de sécurisation des données (voir la fiche n°6 « Les bonnes pratiques en termes de sécurité des données »).
Les avocats doivent ainsi être vigilants quant au niveau de conformité au RGPD de tout logiciel et/ou prestataire choisi pour traiter les données RH des collaborateurs, par exemple les messageries et outils de visioconférence dont l'usage est imposé par le cabinet ou encore l'ensemble des applications préinstallées sur les téléphones de fonction, ainsi qu'aux conditions de stockage et de conservation des données, notamment papiers, en interne (rangées dans des armoires fermées à clé, dans des bureaux fermés à clé, dans des espaces d'archives dédiés et cloisonnés [physiques comme numériques], etc.).

En plus des bonnes pratiques de sécurité exposées dans la fiche n°6 du présent guide, les employeurs, pour parfaire la sécurité de ces informations particulières, devront par exemple :

- conditionner l'accès des salariés à leurs bulletins de paie dématérialisés stockés sur des coffres-forts électroniques par une authentification dite « multifacteur » (MFA) avec des login et mot de passe « robustes » couplés à un envoi de code par SMS ou par e-mail ;
- ne pas reporter le numéro de Sécurité sociale sur les contrats de travail ;
- protéger plus que de raison les CV reçus et supprimer potentiellement de la base active ceux des candidats non retenus quelques mois après la fin du recrutement : en effet, si le niveau de sensibilité des informations contenues dans ces documents semble limité par le fait qu'ils contiennent des données personnelles « classiques » (adresse e-mail, adresse postale, numéro de téléphone, etc.), il convient de noter que ces informations ont nécessairement été vérifiées et mis à jour par les candidats et peuvent présenter un point d'entrée direct pour nuire aux personnes concernées (par *phishing*, arnaque par téléphone, usurpation d'identité, etc.) ; etc.

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 (il s'agira généralement de l'exécution du contrat, de l'obligation légale et de l'intérêt légitime)	☐
Respecter le principe de minimisation	☐
Vérifier les dispositifs de contrôle de l'activité du personnel et leur pertinence et informer les personnels de leur éventuelle utilisation	☐
Procéder à la tenue du registre des traitements avec l'ajout de fiches consacrées aux traitements RH	☐
Définir une politique de durée de conservation des données RH	☐
Informer les personnes concernées de la façon dont sont traitées leurs données personnelles conformément aux éléments énoncés aux articles 13 du RGPD	☐
Mettre en place une procédure de réponse en cas de demande d'exercice des droits des personnes concernées	☐

FICHE N° 4
LA GESTION DES FOURNISSEURS ET DES PRESTATAIRES

1. QU'EST-CE QU'UN SOUS-TRAITANT ?

En vertu de l'article 4, alinéa 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 un comptable, un éditeur de logiciel de cabinet en *SaaS*[58] par exemple stockant les données de ses clients dans sa base, un hébergeur de données, etc.

NOTA : certains hébergeurs de données et éditeurs de logiciel en *SaaS* pourraient refuser de se considérer comme sous-traitant en cas de données hébergées sur leurs serveurs intégralement chiffrées et sans possibilité pour ces premiers de les décrypter (absence de clé de déchiffrement). Néanmoins, le fait que ces données soient stockées sur leurs serveurs suffit à considérer qu'il y a bien un traitement de données effectué pour le compte d'un avocat responsable de traitement. En effet, l'article 4 du RGPD considère bien, parmi tous les types d'opération cités (collecte, lecture, etc.), que l'« enregistrement » constitue un traitement de données à part entière (la liste proposée dans l'article n'est d'ailleurs pas limitative).

2. QUE FAIRE EN CAS DE RELATION AVEC UN SOUS-TRAITANT ?

L'article 28, alinéa 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 des clauses spécifiques prévues par le RGPD où doivent figurer :

- l'identité et les coordonnées du responsable de traitement et du sous-traitant ainsi que de leurs éventuels délégués à la protection des données ;
- l'objet ;
- la durée ;

58. *Software as a service*, se dit d'une solution logicielle applicative hébergée dans le *cloud* d'un prestataire et donc exploitée en dehors du cabinet. Le logiciel en *SaaS* est généralement accessible uniquement à l'aide d'une connexion Internet et *via* une authentification plus ou moins forte.

- la nature des opérations réalisées ;
- les finalités des traitements ;
- 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.

NOTA : certains prestataires considèrent qu'ils n'ont pas à lister dans le contrat de sous-traitance les données traitées pour le compte de leurs clients si ces premiers « s'interdisent » d'y accéder, alors même que ces données sont hébergées par eux. Si la responsabilisation des prestataires en ce sens est louable, le fait qu'ils s'interdisent d'avoir accès aux données contenues sur leurs propres serveurs ne signifie pas pour autant qu'ils ne peuvent pas y avoir accès malgré tout et n'enlève en rien au fait que ces données sont bien stockées sur leurs serveurs. Ainsi, toutes les données traitées doivent bien être listées.

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 et pour le compte du responsable du traitement, même en ce qui concerne les flux transfrontières, et uniquement pour la ou les seule(s) finalité(s) définie(s) ;
- la garantie de confidentialité des données ;
- le respect du principe de protection des données dès la conception (*privacy by design*) et de protection des données par défaut ;
- l'obligation pour les personnes autorisées à accéder aux données de respecter la confidentialité de ces dernières ;
- l'aide qu'il doit fournir au responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées (accès, rectification, effacement, opposition, limitation du traitement, portabilité, droit de ne pas faire l'objet d'une décision individuelle automatisée [y compris le profilage]) ;
- 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 (notamment concernant les analyses d'impact, de violations de données et de consultation préalable de l'autorité de contrôle) ;
- 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.

En vertu de l'article 28, alinéa 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* ».

Sur ce sujet, il est renvoyé au modèle de clauses de sous-traitance ainsi qu'au modèle de registre des sous-traitants en annexes du présent guide.

3. QUE FAIRE SI LE CABINET EST DÉJÀ EN RELATION COMMERCIALE AVEC DES SOUS-TRAITANTS ?

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 organisationnelles et techniques mises en place par le sous-traitant, ils devront conclure un avenant au contrat afin de combler les lacunes, s'il y en a.

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 ou au contrat de base si les clauses de sous-traitance sont inexistantes	☐
Cartographier précisément les traitements de données opérés par les sous-traitants et les décrire dans un registre prévu à cet effet	☐

FICHE N° 5
LA GESTION DE LA LUTTE CONTRE LE BLANCHIMENT ET LE FINANCEMENT DU TERRORISME

La réglementation 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, obéissent 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 (articles L. 561-6[59] et R. 561-12[60] du Code monétaire et financier).

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 (article L. 561-5-1 du CMF) et le cas échéant, sur le bénéficiaire effectif au sens de l'article L. 561-2-2 du CMF.

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

Ainsi, concernant une personne physique, physiquement présente aux fins de l'identification au moment de l'établissement de la relation d'affaires, l'avocat doit se voir présenter l'original d'un document officiel en cours de validité comportant la photographie du client et prendre une copie de ce document (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 qu'il ne s'agit pas 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	☐

59. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072026/LEGISCTA000006154830/#LEGISCTA000020196709
60. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072026/LEGISCTA000019266650/#LEGISCTA000021020431

De plus, en application de l'article R. 561-12, les éléments d'information susceptibles d'être recueillis pendant toute la durée de la relation d'affaires peuvent être pour les personnes physiques :

- la justification de l'adresse du domicile à jour au moment où les éléments sont recueillis ;
- les activités professionnelles actuellement exercées ;
- les revenus ou tout élément permettant d'estimer les autres ressources ;
- tout élément permettant d'apprécier le patrimoine.

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/cnb_guide_lutte-contre-blanchiment_3eme_edition.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 du 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, art. L.561-9, I du CMF). La bonne observation des prescriptions réglementaires 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 du 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 du 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° 6
LES BONNES PRATIQUES EN TERMES DE SÉCURITÉ DES DONNÉES

Il est rappelé que l'avocat, en tant que responsable de traitement, a l'obligation, avec ses sous-traitants potentiels, de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (article 32 du RGPD[61]), risque qui sera généralement élevé pour la profession d'avocat au vu notamment des données traitées.

La sécurisation et la confidentialité des données passent concrètement et notamment par des règles strictes d'habilitations et d'accès : les données contenues dans les fichiers ne doivent être consultées que par les seules personnes habilitées à y accéder en raison de leurs missions.

Les dossiers des avocats ne peuvent être communiqués qu'à des personnes autorisées et habilitées, notamment en application de dispositions législatives particulières et sous réserve du respect du secret professionnel.

Parmi les mesures de sécurité élémentaires permettant de concourir au respect de cette obligation, il convient, par exemple, de veiller à ce que chaque personne habilitée à accéder aux données du système d'information du cabinet dispose d'un mot de passe individuel le plus imprédictible possible (entropie)[62] et que les droits d'accès soient précisément définis en fonction des besoins réels.

Si ce type de mesures de sécurité peut être compris par le plus grand nombre et rendu effectif assez simplement, le sujet de la sécurité des données dans son ensemble reste éminemment complexe pour la plupart des professionnels et impliquera probablement l'intervention et l'aide de spécialistes en la matière afin de ne rien laisser au hasard.

De surcroît, la sécurisation d'un système d'information ne pourra être pleinement assurée que si les enjeux de sécurité sont partagés par tous ; ainsi, il est conseillé aux cabinets de sensibiliser les collaborateurs et les salariés en ce sens en consignant ces enjeux dans une charte informatique.

Enfin, parce qu'il est impossible de réduire complètement les risques, notamment informatiques et numériques, l'avocat responsable de traitement peut demander à souscrire à une « police d'assurance cyber » et espérer ainsi être indemnisé en cas d'attaque informatique. Cette indemnisation ne sera possible que si l'avocat répond à plusieurs conditions :

61. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article32

62. Principe issu de la délibération n°2022-100 du 21 juillet 2022 de la Cnil. Sur ce sujet, un webinaire et un dossier complet ont été publiés sur le site Internet de l'autorité nationale de contrôle.

- une plainte devra être déposée au maximum 72 heures après la connaissance de l'atteinte due à l'incident de sécurité[63] ;

NOTA : ce délai est identique à celui de la notification de violation de données en cas de risque pour les droits et libertés des personnes concernées (voir le point 3.2 de la partie II).

- l'avocat préalablement assuré devra prouver avoir été victime d'une atteinte à un système de traitement automatisé de données (STAD)[64] et avoir subi des pertes et des dommages du fait de cette atteinte.

Attention : la possibilité pour un avocat d'être assuré contre les risques cyber est fortement conditionnée aux preuves que le responsable de traitement pourra fournir en termes de conformité au RGPD, et notamment par la mise en place en interne de procédures et mesures de sécurité préalables.

1. POURQUOI LA SÉCURITÉ DES DONNÉES À CARACTÈRE PERSONNEL EST-ELLE 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 violation 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.

Toutes les obligations précitées de conformité se valent, mais la sécurisation des données devrait être en pratique l'une des priorités poursuivies par l'avocat, celui-ci ne devant pas attendre qu'un incident de sécurité ne survienne dans l'exercice de ses fonctions pour renforcer la protection des données personnelles sous sa responsabilité.

Enfin, si l'avocat a recours à des prestataires pour le traitement des données qu'il gère, il devra évaluer en amont la sécurité de ses sous-traitants et plus généralement leur conformité au RGPD (en demandant à vérifier avant la signature de tout contrat leur documentation et en procédant idéalement à des audits).

63. Article L. 12-10-1 du Code des assurances.
64. Au sens des atteintes énumérées aux articles 323-1 à 323-3-1 du Code pénal.

2. QUELLES MESURES DE SÉCURITÉ PHYSIQUES DOIVENT-ELLES ÊTRE MISES EN PLACE ?

Il est nécessaire de mettre en place des mesures de sécurité **physiques** dans votre cabinet, et parmi elles :

- 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 et dans des espaces de rangement non fermés à clé ;
- installer des alarmes dans les locaux du cabinet ;
- déployer, si ceci est pertinent et proportionné (exemple : locaux relativement étendus, passage de visiteurs important, etc.) des caméras de vidéosurveillance pour sécuriser les accès et dissuader toute intrusion ou autre acte malveillant et illicite (la vidéosurveillance participe à protéger les données personnelles à travers la sécurisation des biens du cabinet et notamment l'accès physique à l'outil informatique). Toutefois, différentes précautions doivent être prises avant l'installation de tels dispositifs (notamment de ne pas filmer les employés sur leur poste de travail) ;
- ne pas laisser de documents concernant les clients à la vue et à portée de main d'autres personnes non autorisées ; etc.

3. QUELLES MESURES DE SÉCURITÉ LOGIQUES/NUMÉRIQUES DOIVENT-ELLES ÊTRE MISES EN PLACE ?

Il est nécessaire de mettre en place des mesures de sécurité logiques dans votre cabinet, et parmi elles :

- **authentifier les utilisateurs de manière forte :**
  - mettre en place pour l'accès à tous les espaces numériques (ordinateur de bureau/portable, logiciel, application accessible par navigateur Internet, site Internet de l'avocat, etc.) une authentification *via* un mot de passe présentant un degré de complexité fort (l'entropie) et non plus une longueur minimale afin d'offrir plus de liberté dans la définition de politiques de mots de passe robustes[65] et adaptées aux cas d'usage (conformément à la nouvelle recommandation relative aux mots de passe publiée par la Cnil en 2022, cf. *supra*).

    Il convient de doubler la connexion login/mot de passe avec une authentification dite « multifacteur » (dit « MFA », code de confirmation reçu par SMS ou par e-mail à la suite d'une authentification classique réussie).

  - ne pas partager le mot de passe,
  - ne pas le noter en clair sur une feuille ou un post-it (et plus généralement, ne jamais le stocker en clair),

65. Pour information, France Num présente pour 2023 dans un tableau complet le temps qu'un pirate pourrait mettre à deviner votre mot de passe en fonction de sa longueur et de ses caractéristiques.

- éviter au maximum de l'enregistrer dans un navigateur Internet par exemple,
- le modifier « réellement » (changement total de la suite de caractères et interdiction de reprise du précédent mot de passe agrémenté d'un caractère au début ou à la fin par exemple) uniquement en cas de doutes, avérés ou non, sur une perte de confidentialité des informations détenues par l'avocat.

> **NOTA :** la Cnil ne préconise plus désormais le renouvellement périodique des mots de passe (sauf pour les comptes administrateurs) et préconise plutôt le choix d'un mot de passe présentant un haut degré de complexité (l'entropie [66]) pour ne plus avoir à en changer.

- **gérer les habilitations et sensibiliser les utilisateurs :**
  - identifier les personnes habilitées à accéder aux données à caractère personnel,
  - vérifier périodiquement les habilitations en application et supprimer les permissions d'accès obsolètes,
  - rédiger une charte informatique et l'annexer au règlement intérieur lorsqu'il en existe un, interdisant notamment le téléchargement de logiciel non autorisé ou autres outils disponibles en ligne et décider de la conduite à tenir lorsque le personnel accède au système informatique du cabinet par des appareils privés (BYOD [*Bring your own device*], ou en français AVEC [Apportez votre équipement personnel de communication]) formalisée par la mise en place d'une politique particulière.
- **sécuriser les envois et les échanges de pièces :**
  - entre avocats, et entre avocats et clients…
  - … par exemple au moyen de plateformes sécurisées plutôt que par l'envoi d'e-mails en clair, présentant des risques en termes de sécurité (sauf si ces e-mails sont chiffrés).
- **sécuriser l'informatique mobile :**
  - prévoir des moyens de chiffrement pour les ordinateurs portables et les serveurs de stockage,
  - chiffrer les données stockées, notamment les dossiers des clients,
  - chiffrer les matériels de stockage amovibles (clés USB, disques durs amovibles, etc.) et verrouiller leur accès par des mots de passe ou systèmes de blocage (dans la négative, ne pas utiliser ce type de matériel pour stocker les données à caractère personnel sensibles des clients ou du personnel), etc.
- **sauvegarder et prévoir la continuité d'activité :**
  - mettre en place des sauvegardes régulières et « hors ligne » (et en dehors de l'espace de stockage principal),
  - stocker les supports de sauvegarde dans un endroit sûr ;
- **appliquer le plus régulièrement possible les mises à jour, correctifs et installations de patchs de sécurité des logiciels, applications et systèmes d'exploitation utilisés.**

66. Pour tester le niveau d'entropie de son mot de passe, la Cnil propose cet outil : https://www.cnil.fr/fr/verifier-sa-politique-de-mots-de-passe.

- **vérifier les prestataires informatiques et numériques avant tout recours à leurs services :**
  - demander les garanties de sécurité appliquées par le fournisseur de service en fonction ainsi que des preuves de documentation de sa propre conformité au RGPD (article 28.1 du RGPD),
  - évaluer les mesures de sécurité techniques et organisationnelles en fonction de la sensibilité des données en jeu et du niveau de risque, etc,
  - privilégier des prestataires détenant des serveurs de stockage de données situés en France ou dans l'Union européenne (sans pour autant négliger le niveau de sécurité offert), surtout si les données hébergées peuvent être qualifiées de « sensibles », et informer les clients du recours à ces prestataires ;
- spécifiquement, **ne pas utiliser d'applications en ligne de détection d'antivirus/malwares pour des fichiers, notamment contenant des éléments de procédures, ou bien de conversion de fichiers (Word en PDF par exemple) :** hormis si vous êtes absolument sûr du service utilisé, cette pratique peut se révéler dangereuse car elle induit un téléversement (*upload*) de vos fichiers sur des serveurs distants sans aucune possibilité de maîtrise future ;
- **gérer l'effacement effectif des données et la destruction des documents avec des prestataires de confiance, etc.**

4. COMMENT NOTIFIER ET COMMUNIQUER AU SUJET D'UNE VIOLATION DES DONNÉES À CARACTÈRE PERSONNEL ?

La notification à l'autorité de contrôle en cas de violation de données ayant entraîné un risque pour les droits et libertés des personnes concernées doit être réalisée dans les 72 heures après la prise de connaissance de la violation par l'avocat (voir le point 3.2 de la partie II).

L'avocat peut procéder à une notification d'une violation de données en ligne sur le site Internet de la Cnil : https://notifications.cnil.fr/notifications/index.

En cas de risque élevé pour les personnes concernées, l'avocat devra procéder « dans les meilleurs délais » à une communication aux personnes concernées. L'avocat devra cependant s'interroger préalablement sur les conditions de réalisation d'une telle communication sans manquer par ailleurs à son obligation de confidentialité.

La survenance de toute violation de données, même sans risque pour les personnes, doit être obligatoirement consignée dans un document, tel un registre dédié (voir le point 3.2 de la partie II ainsi que le modèle de registre de violation de données en annexe).

5. LES RÈGLES DE SÉCURITÉ DU CABINET S'APPLIQUENT-ELLES DE LA MÊME MANIÈRE POUR LES COLLABORATEURS LIBÉRAUX ?

Comme évoqué, le cabinet est tenu d'assurer la sécurité et la confidentialité des dossiers du client en mettant en place les « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque » (article 32 du RGPD).

Le statut libéral du collaborateur ne justifie aucune dérogation, ce dernier est soumis à l'éventuelle charte d'utilisation des ressources informatiques du cabinet comme n'importe quel autre membre de l'entreprise. Au titre de l'article 32 précité, le cabinet doit également s'assurer du respect des règles de sécurité applicables.

Concernant ses dossiers personnels, le collaborateur peut fixer ses propres règles de sécurité, à condition de le faire dans les règles de l'art technique (donc avec un professionnel) et d'en informer préalablement son responsable afin d'éviter la présence de conflits de sécurité.

Cependant, le cabinet doit veiller à ce que le prestataire retenu possède des garanties de sérieux nécessaires à la sauvegarde de la sécurité du réseau du cabinet. Le collaborateur s'assurera par ailleurs du respect de la confidentialité par le prestataire (signature d'un accord de confidentialité) et de la restriction de l'accès à distance au réseau du cabinet par le suivi et la traçabilité des droits d'accès.

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	☐
- Installer (éventuellement) des caméras de vidéosurveillance	☐
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	☐
- Vérifier les prestataires informatiques et numériques avant tout recours à leurs services	☐
Mettre en place une charte informatique	☐
Mettre en place des procédures de notification de violations de données personnelles	☐

Il est rappelé que la Cnil a publié un guide, mis à jour en 2023, retraçant 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**.

Enfin, la directive européenne *Network and Information Security 2* (NIS2), publiée au *Journal officiel de l'Union européenne* le 27 décembre 2022, a élargi le champ d'application de la précédente directive NIS1 qu'elle a abrogée, et a pour objectif de renforcer le régime de cybersécurité de l'Union en augmentant son niveau, et ce pour de nouveaux secteurs. La directive devra être transposée notamment dans le droit français avant la fin d'année 2024, précisément le 17 octobre au plus tard.

FICHE N° 7
LA GESTION DE LA VIDÉOSURVEILLANCE/ VIDÉOPROTECTION

1. QU'EST-CE QUE LA VIDÉOSURVEILLANCE ET LA VIDÉOPROTECTION ?

Selon le lieu où les caméras sont installées et son mode d'accès, 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 sans mesure de filtrage à l'entrée, 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 non ouvertes au public et réservées aux membres du cabinet et à leurs clients habilités à y accéder, comme les bureaux, les réserves, les couloirs du cabinet d'avocats, etc. Quel que soit le régime applicable, la Cnil est compétente pour opérer des contrôles sur les dispositifs déployés.

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 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 ce sens, le recours à la vidéoprotection ou à la vidéosurveillance ne sera pas nécessairement adapté à tous les cabinets d'avocats, seuls ceux dont l'activité permet de considérer qu'il existe un risque pour la sécurité des personnes ou des biens devraient pouvoir s'équiper de tels dispositifs (proportionnalité), sous réserve du respect de l'ensemble des principes fondamentaux issus du RGPD.

En vertu du droit au respect de la vie privée (article 9 du Code civil), la vidéosurveillance ne peut en aucun cas servir, même de manière officieuse, à surveiller les collaborateurs et personnels, voire ses clients ou visiteurs occasionnels. Ainsi, il est interdit de filmer les membres du cabinet sur leur poste de travail, dans les zones de pause ou de repos, dans un couloir ne menant qu'aux toilettes ou encore dans les éventuels locaux des représentants du personnel.

3. QUELLES SONT LES FORMALITÉS À ACCOMPLIR ?

Les dispositifs de vidéoprotection et de vidéosurveillance sont très encadrés et ne doivent être mis en œuvre respectivement qu'après l'accomplissement de certaines formalités ou après vérification et application méticuleuse des principes fondamentaux du RGPD et de la loi Informatique et libertés appliqués au déploiement et aux conditions de collecte et de traitement des données issues de la captation.

Concernant la vidéoprotection, si les caméras sont soumises aux dispositions du Code de la sécurité intérieure (le dispositif devrait *a priori* concerner un nombre de cas plutôt limité, comme celui du « hall d'entrée » d'un cabinet dès lors qu'il pourra être considéré comme étant un lieu auquel le public a accès sans filtrage particulier), une autorisation de la préfecture du département (préfet de police pour Paris) sera alors nécessaire (art. L. 251-1 et suivants du Code de la sécurité intérieure).

Concernant la vidéosurveillance, les caméras sont soumises aux dispositions du RGPD et de la LIL.

TYPE DE DISPOSITIF	EXEMPLE	FORMALITÉS À ACCOMPLIR
La caméra est située dans le cabinet d'avocats non ouvert au public	Réserves, salle de reprographie, couloirs du cabinet d'avocats, etc.	Aucune formalité préalable si ce n'est la vérification que les principes fondamentaux de la protection des données sont bien respectés + ajout du traitement dans le registre + potentielle étude d'impact à mener + vérification du contrat et des clauses de sous-traitance avec le prestataire
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	Abords de l'immeuble du cabinet d'avocats, hall d'accueil sans mesure de filtrage, parking accessible par des piétons, etc.	Autorisation préfectorale + vérification que les principes fondamentaux de la protection des données sont bien respectés + ajout du traitement dans le registre + potentielle étude d'impact à mener + vérification du contrat et des clauses de sous-traitance avec le prestataire
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		

Quelle que soit la situation, le traitement de données doit être ajouté au **registre des activités de traitement** par l'insertion d'une fiche dédiée à la vidéosurveillance/vidéoprotection dans le registre des traitements (voir le point 3.1 de la partie II).

Une analyse d'impact sur la vie privée pourrait également être menée (analyse au cas par cas en fonction du traitement envisagé[67]), plusieurs critères tendant à s'appliquer (voir le point 3.2 de la partie I) :

- surveillance constante (potentiellement) ;
- personnes vulnérables (potentiellement), par exemple les salariés ou des clients en situation de précarité.

NOTA : le critère de l'utilisation d'une nouvelle technologie innovante semble aujourd'hui ne plus correspondre, en l'état de la technique et des risques, à une caméra vidéo « simple » (contrairement à des caméras « augmentées », équipées ou non de système de reconnaissance faciale par exemple).

4. COMMENT 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 informées 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[s] de l'établissement). Cette information doit porter *a minima* sur les éléments demandés par l'article 13 du RGPD (voir le point 3.1.5.1. de la partie I). 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, conforme donc aux exigences du RGPD (cf. *supra*).

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 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.

67. Des critères d'analyse ont été précisés et diffusés pour aider les responsables de traitement à réaliser cet examen (Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) [...]).

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, 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.

7. LES MESURES DE SÉCURITÉ

Au vu des risques inhérents à de tels traitements, les avocats doivent s'évertuer à sécuriser au maximum les données collectées et stockées dans ce cadre. Outre un accès par habilitation stricte et une suppression récurrente des données (sans incident à 7 ou 14 jours, sans dépasser 30 jours) qui diminuent le risque d'accès illégitime à une donnée, la solution retenue doit respecter le principe de *privacy by default* (voir le point 3.2 de la partie I) et devrait présenter certaines caractéristiques :

- authentification forte pour accéder aux images (voir la fiche n°6 « Les bonnes pratiques en termes de sécurité des données ») ;
- stockage en local des données sans que le système soit relié à l'Internet avec protection accrue de ce système de stockage ;
- encadrement des éventuels transferts de données en dehors de l'Union européenne ;
- impossibilité pour les personnels du prestataire d'accéder aux images de la vidéosurveillance, même en cas de maintenance (si possible) ;
- irréversibilité de la suppression des images une fois le délai fixé ou légal dépassé, etc.

Si une procédure judiciaire était engagée, les images doivent pouvoir être extraites du dispositif (après consignation de cette opération dans un cahier/registre spécifique) et conservées pour la durée de la procédure.

8. EST-IL NÉCESSAIRE DE VÉRIFIER LE CONTRAT DE PRESTATION ?

Il est fort probable que le déploiement des caméras implique le recours à un prestataire souvent chargé de la maintenance et du stockage des données. Dans cette situation, l'entreprise sollicitée sera alors considérée comme le sous-traitant (voir la fiche n°4 « La gestion des fournisseurs et prestataires ») de l'avocat responsable de traitement.

Ainsi, si le prestataire est amené à traiter des données relatives au traitement de vidéosurveillance/vidéoprotection pour le compte du cabinet, le contrat qui lie les deux entités doit être conforme à l'article 28 du RGPD et contenir des clauses de sous-traitance.

L'avocat responsable de traitement a l'obligation de choisir un sous-traitant présentant toutes les garanties suffisantes de sécurité et de conformité globale au RGPD.

THÈME	À FAIRE	
Général	Identifier les caméras	☐
	Déterminer la localisation des caméras et les lieux filmés et les formaliser dans un plan d'emplacement des caméras	☐
	Limiter l'accès aux images enregistrées	☐
	Constituer la fiche de traitement de vidéosurveillance/ vidéoprotection et l'inscrire dans le registre des activités de traitements	☐
	Afficher un panneau visible dans les lieux et locaux concernés et à chaque entrée	☐
	Consulter les instances représentatives du personnel avant l'installation des caméras, le cas échéant	☐
	Informer individuellement les collaborateurs et le personnel le cas échéant (notamment par courriel)	☐
	Limiter la durée de conservation des images à un mois au maximum	☐
	Créer un registre des consultations et éventuelles extractions des images	☐
	Mettre en place des mesures de sécurité techniques et organisationnelles (en lien avec le prestataire) maximales (notamment l'habilitation des membres du cabinet autorisés à visionner les images ainsi qu'une trace de leur sensibilisation à ce sujet)	☐
	Vérifier la conformité au RGPD du contrat avec le prestataire ayant déployé les caméras et la présence de clauses de sous-traitance si besoin	☐
Vidéoprotection	Procéder à une demande d'autorisation auprès de la préfecture du département	☐
Vidéosurveillance	Orienter les caméras de façon à ne pas filmer continuellement les personnels (par exemple à l'accueil, la caméra peut ne « voir » que le comptoir et la ou les personne[s] s'y présentant, et non le salarié derrière)	☐
	Effectuer une analyse d'impact sur la protection des données relative au dispositif en fonction de la situation	☐

Pour en savoir plus :
https://www.cnil.fr/sites/default/files/atoms/files/_videosurveillance_au_travail.pdf

FICHE N° 8
LA GESTION DES ACCÈS PHYSIQUES

Sur le lieu de travail, les avocats agissant en qualité d'employeur peuvent être amenés à contrôler les accès aux locaux ou la gestion de la restauration (*via* par exemple des badges électroniques). 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

D'une manière générale, l'avocat responsable de traitement, doit, avant tout traitement de données de gestion des accès physiques, s'assurer que le recours à un dispositif de contrôle dans ce cadre n'est pas disproportionné et veiller à ce que le personnel du cabinet ne soit pas soumis à une surveillance constante.

Pour ce faire, les systèmes de contrôle d'accès utilisés seront généralement des badges, accompagnés potentiellement de digicodes et de clés. Les badges électroniques (cartes magnétiques ou à puce) peuvent ainsi 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 à ces personnes faisant l'objet d'une collecte et d'un traitement de leurs données personnelles, notamment le respect par l'avocat responsable de traitement du principe de minimisation par lequel seules les informations strictement nécessaires au traitement sont collectées et en évitant les technologies « gourmandes » en termes de données.

Chaque passage du badge dans un lecteur peut, selon le paramétrage, permettre 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, etc.) ;
- les informations collectées ;
- les services destinataires des données (poste de sécurité ? service RH ? direction ? autre ?) ;
- les hypothèses dans lesquelles ces services peuvent accéder aux données (contrôles réguliers ? audits occasionnels ? faisant suite à un signalement ? etc.)
- la durée de conservation des informations (avec mise en place d'une procédure de suppression automatisée une fois la durée de conservation atteinte [3 mois au maximum]) ;
- 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.

Sur ce sujet, les cabinets d'avocats peuvent se référer aux préconisations de la Cnil pour ce type de traitement : **https://www.cnil.fr/fr/lacces-aux-locaux-et-le-controle-des-horaires-sur-le-lieu-de-travail**.

2. LES DISPOSITIFS BIOMÉTRIQUES

D'une manière générale, la gestion des accès peut intervenir 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, iris de l'œil, etc., voire la démarche).

La Cnil reconnaît que « *la biométrie est [...] une alternative plus ergonomique et plus fiable que le port de badges encombrants et que l'on peut oublier,* [qui permet] *de reconnaître automatiquement les personnes et* [repose] *sur une réalité biologique permanente, dont* [les personnes] *ne peuvent s'affranchir* ». Mais, dans un même temps, l'article 9 du RGPD considère ce type de données comme « particulière » (sensible), *« le mauvais usage ou le détournement d'une telle donnée [pouvant] alors avoir des conséquences graves pour les droits et libertés des personnes »,* comme le conclut l'autorité de contrôle.

Le traitement de ce type de données dites « sensibles » 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 sur ce sujet début 2019 un **règlement type** relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail, dit « biométrie sur les lieux de travail », revêtant un caractère contraignant.

3. COMMENT SAVOIR SI LE RECOURS À UN SYSTÈME BIOMÉTRIQUE DE CONTRÔLE DES ACCÈS EST PERTINENT ?

La première étape de conformité consiste d'emblée à se demander si le recours au traitement de données biométriques est nécessaire ; pour ce faire, la Cnil suggère que les responsables de traitement se posent un certain nombre de questions préalables, et par exemple :

- un système de badge « classique » est-il suffisant ?
- le projet de système biométrique ne répond-il qu'à un besoin de confort ou d'affichage extérieur ?
- les locaux, applications ou appareils protégés sont-ils particulièrement sensibles ?

Si la réponse est positive, le traitement biométrique ne semble pas approprié, une solution moins intrusive et moins risquée pour les droits et libertés des personnes doit être privilégiée en conformité avec la réglementation.

Si la réponse est négative, la seconde étape de conformité sera de rendre effectif un traitement de données biométriques dans ce cadre :

- justification écrite et preuve de conformité du recours à un traitement de données biométriques, en indiquant dans un document les raisons pour lesquelles d'autres dispositifs d'identification (badges, mots de passe, etc.) ne seraient pas suffisants ainsi que le type de données biométriques retenu pour authentification plutôt qu'un autre ;
- vérification, choix et maîtrise du système de stockage en fonction des données du corps humain en jeu ;
- transformation des données biométriques collectées initialement en données biométriques « dérivées » (gabarits chiffrés) et suppression définitive dans la foulée des données originelles ;
- effacement strict des données ne devant pas dépasser les délais de conservation fixés par le règlement type (durée d'habilitation pour les gabarits, six mois pour les logs de connexion [journalisation], etc.) ;
- mesures maximales de sécurité, aussi bien sur le plan technique qu'organisationnel ;
- réalisation d'une analyse d'impact (voir le point 3.2 de la partie I), obligatoire en cas de mise en œuvre d'un traitement de données biométriques.

Le règlement type de la Cnil précité énonce clairement que les dispositifs de contrôle d'accès biométrique ne peuvent être mis en place que là où ils sont « nécessaires ». Ce faisant, les cas d'usage où cette condition est remplie sont très rares.

Le recours à ce type de dispositifs, devant rester purement exceptionnel, ne semble pas, en tout état de cause, s'appliquer aux cabinets d'avocats. Ces derniers doivent privilégier des moyens de contrôle des accès éprouvés tels les badges électroniques, suffisant *a priori* pour sécuriser les locaux du cabinet.

À FAIRE	
Vérifier la nécessité de recours à un moyen de contrôle, par exemple par badge, et veiller à rechercher des dispositifs ne collectant que des données strictement nécessaires à la réalisation de la finalité (minimisation)	☐
Effectuer une analyse d'impact sur la vie privée le cas échéant	☐
Informer les personnes concernées de la mise en place d'un dispositif de contrôle des accès	☐
Ajouter, le cas échéant, une fiche de traitement au registre en cas de recours à un dispositif de contrôle des accès physiques	☐

FICHE N° 9
LA MISE EN CONFORMITÉ DU SITE 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 ;
- un abonnement à une lettre d'information/*newsletter* ;
- la création d'un compte en ligne ;
- des cookies, etc.

Les avocats, laissant la plupart du temps le soin à une société spécialisée de construire leur site Internet, doivent être vigilants quant au choix du prestataire retenu et doivent vérifier que ce dernier, outre les garanties suffisantes qu'il présente, connaisse les aspects de conformité d'un site Internet,

1. QUELLES SONT LES FORMALITÉS À ACCOMPLIR SI L'AVOCAT COLLECTE DES DONNÉES À CARACTÈRE PERSONNEL *VIA* SON SITE INTERNET ?

Le RGPD, comme indiqué précédemment, a grandement allégé les formalités mais introduit, en contrepartie, de nouvelles obligations pour le responsable de traitement.

Un premier réflexe pour l'avocat sera de renseigner les traitements de données liés à la gestion du site Internet dans des fiches de traitement potentiellement ajoutées au **registre des activités de traitement.** Celui-ci répertorie les informations relatives aux caractéristiques des traitements mis en œuvre par le responsable de traitement (voir le point 3.1 de la partie II).

Il convient donc d'insérer dans le registre des activités de traitement les fiches correspondant aux traitements de données opérées sur le site Internet dont vous trouverez des modèles en annexe.

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 (LCEN) ;
- 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) ;
- les mentions d'informations issues des articles 13 et 14 du RGPD ;
- les mentions d'informations relatives aux cookies et autres traceurs.

Attention : pour satisfaire aux conditions de forme de l'obligation de transparence et d'information énoncée à l'article 12 du RGPD, les mentions d'information RGPD et celles relatives aux cookies (traceurs, cf. *infra*) doivent être présentées dans des espaces dédiés, *a minima* des pages uniques, et ne pas être diluées et mélangées aux mentions légales générales issues de la LCEN. En effet, la personne concernée souhaitant connaître les modalités de traitement et le « devenir » de ses données ne devrait pas avoir à « fouiller » sur le site ou au sein des mentions légales, les informations devant lui être apportées simplement par la présence de pages dédiées à ces questions.

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)
		Éléments 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 (dans une page dédiée pouvant s'intituler « Politique de confidentialité », « Gestion de la protection des données/de la vie privée », « Données personnelles », etc.)	Articles 13 et 14 du RGPD Article 104 de la loi Informatique et libertés	L'identité et les coordonnées du responsable du fichier
		Les coordonnées du délégué à la protection des données s'il existe ou, *a minima*, d'une adresse dédiée aux questions de protection des données et d'exercice des droits RGPD
		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
		Le caractère obligatoire ou facultatif des données collectées et les conséquences en cas de non-fourniture des données pour l'utilisateur
		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
		Des informations sur la question de savoir si l'exigence de fourniture des données a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat (article 13.2.e du RGPD)

MENTIONS	TEXTES	INFORMATIONS
Mentions d'information relatives aux cookies (dans une page dédiée pouvant s'intituler « Politique de cookies », « Gestion des cookies », etc., et/ou rattachée au système de gestion des consentements	Les directives du 25 novembre 2011 dites « Paquet télécom » 2009/136/CE et 2009/140/CE Ordonnance « Paquet télécom » du 24 août 2011 Directive 2002/58/CE du 12 juillet 2002 : l'article 5(3) a posé le principe : • d'un consentement préalable de l'utilisateur avant le stockage d'informations sur son terminal ou l'accès à des informations déjà stockées sur celui-ci ; • sauf si ces actions sont strictement nécessaires à la fourniture d'un service de communication en ligne expressément demandé par l'utilisateur ou ont pour finalité exclusive de permettre ou faciliter une communication par voie électronique. Article 82 de la Loi du 6 janvier 1978 : **a transposé les dispositions ci-dessus en droit français.** Les lignes directrices et recommandations de la Cnil du 17 septembre 2020 : complétées par une recommandation visant notamment à proposer des exemples de modalités pratiques de recueil du consentement Le projet de règlement européen « e-Privacy »	Les finalités des cookies Le recueil du consentement des utilisateurs *via* « les bandeaux de consentement » pour certains types de cookies (cf. *infra*) Les possibilités de refus des cookies

4. AI-JE BESOIN DU CONSENTEMENT DE MES CLIENTS POUR LEUR ENVOYER UNE *NEWSLETTER* D'INFORMATION OU UNE SOLLICITATION PERSONNALISÉE ?

Il n'est pas obligatoire pour l'avocat de recueillir le consentement de ses clients pour leur transmettre une lettre d'information relative aux actualités du cabinet et aux services dispensés, ce traitement étant basé sur l'intérêt légitime du responsable de traitement et couvert par les énonciations de l'article L. 34-5 du Code des postes et des communications électroniques [68].

En revanche, toute transmission à des particuliers non clients du cabinet ne doit pouvoir se faire qu'avec le consentement préalable (consentement conforme aux énonciations de l'article 7 du RGPD [69]) des personnes concernées.

68. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042155961.
69. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article7.

S'il s'agit de professionnels, la Cnil estime de manière doctrinale que le consentement n'aura pas à être recueilli préalablement mais uniquement si les communications sont transmises à des personnes dont la profession est en rapport avec la sollicitation (par exemple les membres de la direction juridique d'une entreprise).

Attention : dans n'importe quel cas, au moment du recueil de l'adresse courriel utilisée à des fins de prospection, l'information doit être fournie aux personnes concernées (voir le point 3.1.5.1. de la partie I) et un lien de désinscription devra obligatoirement être inséré sur la lettre d'information (pour satisfaire à l'exercice du droit d'opposition).

À cet égard, un vade-mecum de la communication des avocats est disponible sur le site Internet du Conseil national des barreaux.

5. COMMENT RENDRE CONFORME L'UTILISATION DES COOKIES SUR LE SITE INTERNET DE L'AVOCAT ?

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, etc.

Les cookies et autres traceurs ont généralement pour finalités d'analyser la navigation et la fréquentation du site Internet du cabinet d'avocats, de sécuriser le site Internet, etc.

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

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 et d'autres non :

- Cookies (tiers) nécessitant le consentement préalable à l'insertion ou à la lecture de cookies (tant que le client n'a pas donné son consentement par un acte positif clair et sans ambiguïté, ces cookies ne peuvent être déposés ou lus sur son terminal), sachant que ce consentement doit être gardé en mémoire (preuve du consentement) et doit pouvoir être révoqué à tout moment et aussi simplement (réversibilité) :
  - les cookies publicitaires ;
  - les cookies de « réseaux sociaux », générés par les boutons de partage lorsqu'ils collectent des données personnelles sans consentement des personnes concernées ;
  - les cookies de sites de vidéos en ligne ;
  - les cookies de géolocalisation ;
  - certains cookies de mesure d'audience ; etc.

- Cookies (techniques) ayant pour finalité exclusive de permettre ou faciliter une communication par voie électronique ou étant strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur, ne nécessitant pas à l'inverse de consentement :
  - les cookies de sécurité ;
  - les cookies de session ;
  - les cookies conservant le choix exprimé par les utilisateurs sur le dépôt de traceurs ;
  - les cookies de personnalisation de l'interface utilisateur (par exemple pour le choix de la langue) et lorsqu'une telle personnalisation constitue un élément attendu du service ;
  - certains cookies de mesure d'audience s'ils respectent certaines conditions [70].

NOTA : l'avocat comprend ainsi que, en fonction d'un certain nombre de paramètres [71], un cookie de mesure d'audience peut être exempté de consentement.

Enfin, la configuration d'un système de recueil du consentement pour le dépôt de cookies et autres traceurs doit désormais répondre à certaines règles, et notamment :

- la simple poursuite de la navigation sur un site ne peut plus être considérée comme une expression valide du consentement de l'internaute ;
- les personnes doivent consentir au dépôt de traceurs par un acte positif clair et, si elles ne le font pas, aucun traceur non essentiel au fonctionnement du service ne pourra être déposé sur leur appareil ;
- les utilisateurs devront être en mesure de retirer leur consentement, facilement, et à tout moment ;
- refuser les traceurs doit être aussi aisé que de les accepter ;
- l'interface de recueil du consentement ne doit pas seulement comprendre un bouton « tout accepter » mais aussi un bouton « tout refuser ».
- chaque acteur se prévalant du consentement doit être en mesure d'en apporter la preuve ;
- concernant l'information des personnes, ces dernières doivent clairement être informées des finalités des traceurs avant de consentir, ainsi que des conséquences qui s'attachent à une acceptation ou un refus de traceurs ;
- Les sites Internet, qui généralement conservent pendant une certaine durée le consentement aux traceurs, doivent également garder en mémoire le refus des internautes pendant une certaine période afin de ne pas réinterroger l'internaute à chacune de ses visites ; etc.

70. Liste de traceurs considérés comme techniques fournie par la Cnil : **https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies-solutions-pour-les-outils-de-mesure-daudience** (cette liste ne tient pas compte des restrictions en matière de transfert international de données).

71. Sur ce sujet, voir la **délibération n°2020-091 du 17 septembre 2020** de la Cnil, page 9

La Cnil a publié sur son site Internet un certain nombre d'articles récapitulatifs à ce sujet :
https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/que-dit-la-loi
https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/FAQ
https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/lignes-directrices-modificatives-et-recommandation

À FAIRE	
Intégrer des mentions légales et obligatoires	☐
Intégrer des mentions RGPD dans un encart dédié et facilement trouvable	☐
Ajouter des fiches de traitement dans le registre des activités de traitements (gestion du formulaire de contact, gestion de l'abonnement à la *newsletter*, gestion des statistiques de visite du site Internet, etc.)	☐
Identifier la présence de cookies mis en place sur le site Internet de l'avocat	☐
Identifier le type de cookies présents sur le site Internet	☐
Mettre en place un bandeau de recueil du consentement en cas d'utilisation de cookies tiers (non techniques) avec la configuration suivante, et notamment[72] : - un blocage du dépôt du ou des traceur(s) nécessitant le recueil du consentement sur le terminal de l'utilisateur par une simple poursuite de la navigation, - la présence d'une information claire indiquant notamment les finalités des cookies **déposés** et la liste des responsables des traitements opérés *via* ces cookies, - des boutons d'acceptation et de refus similaires au même endroit (par exemple de mêmes taille et visibilité de façon à ne pas tromper l'utilisateur), etc.	☐
Intégrer des mentions d'information sur les cookies dans un encart dédié et facilement localisable	☐

72. Sur ce sujet, voir la publication de la Cnil « Questions-réponses sur les lignes directrices modificatives et la recommandation « cookies et autres traceurs » de la Cnil ».

FICHE N° 10
LES TRANSFERTS DE DONNÉES HORS UNION EUROPÉENNE EN CAS DE RECOURS À DES PRESTATAIRES NUMÉRIQUES

Le principe au sein de l'Union européenne (UE) de la libre circulation des données sans formalités particulières assure une fluidité du déplacement des données dans un espace défini et sécurisé. Cette sécurité est assurée par l'application commune du RGPD par tous les États membres, définissant un niveau de protection des données équivalent dans toute l'Union ainsi que pour les autres États membres de l'Espace économique européen (Islande, Lichtenstein, Norvège).
Mais une telle protection n'est *a priori* pas garantie dans les États n'appartenant pas à ces espaces, qualifiés de « pays tiers ».

1. QUELLES SONT LES MODALITÉS DE TRANSFERT DE DONNÉES PERSONNELLES EN DEHORS DE L'UE ET DE L'EEE ?

Le transfert de données vers des pays extérieurs est par principe interdit sauf cas particuliers prévus par la réglementation. L'article 44 du RGPD[73] énonce qu'un transfert de données ne sera licite que s'il entre dans les conditions et exceptions prévues aux articles suivants :

- le transfert peut être fondé sur une décision d'adéquation bénéficiant au pays de l'importateur des données (article 45 du RGPD[74]). Cette décision permet le transfert de données vers le destinataire aussi simplement que s'il s'agissait d'un État membre de l'UE.
  Les pays considérés comme offrant un niveau de protection adéquat sont par exemple le Royaume-Uni, le Japon, la Nouvelle-Zélande, Andorre, la Corée du Sud, l'Argentine, Israël, etc. ;
- le transfert peut être mis en œuvre si des « garanties appropriées » sont mises en place avec l'importateur des données (article 46 du RGPD[75]), à savoir celles ne nécessitant pas l'autorisation de l'autorité de contrôle : règles d'entreprise contraignantes, clauses contractuelles types de la Commission européenne ou CCT (dans leur version publiée le 4 juin 2021), etc. ; et celles pour lesquelles cette formalité est requise comme des codes de conduite, des clauses contractuelles types adoptés par une autorité de contrôle, des certifications, etc ;

73. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre5#Article44.
74. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre5#Article45.
75. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre5#Article46.

- à titre exceptionnel le transfert peut se faire sur la base d'une dérogation prévue à l'article 49.f du RGPD[76] si le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice.

Le transfert et l'hébergement appellent dans ce cadre aux respects des dispositions générales auxquelles devront s'ajouter des garanties contractuelles supplémentaires pour veiller aux respects des obligations professionnelles et déontologiques des avocats.

2. QUELS SONT LES POINTS D'ATTENTION CONCERNANT LE CHOIX D'UN PRESTATAIRE SITUÉ EN DEHORS DE L'UE ET DE L'EEE ?

L'avocat devra prêter une attention toute particulière au choix de son prestataire et cela pour s'assurer du respect du secret professionnel, des règles relatives au conflit d'intérêts ou encore des règles concernant le blanchiment. Il doit être vigilant sur le plan contractuel.

Pour des questions de gouvernance des données, le transfert de données personnelles en dehors de l'UE devrait être écarté chaque fois que cela est possible. Il est ainsi conseillé pour l'avocat de vérifier que les sous-traitants qu'il sollicite prévoient des hébergements de données au sein de l'Union, voire en France, sans aucun transfert en dehors de ce cadre avec leurs éventuels sous-traitants (ultérieurs).

En pratique, ceci peut s'avérer compliqué si le professionnel décide d'avoir recours à des prestataires américains, notamment informatiques et numériques (comme les GAMAM[77]), dominants sur le marché et présentant généralement un intérêt en termes de disponibilité et de sécurisation des données.
Dans ce cadre, les transferts de données de l'Union européenne vers les États-Unis (USA) ont été remis en cause depuis l'invalidation du mécanisme d'autocertification pour les sociétés établies aux États-Unis dit du « Privacy Shield », reconnu auparavant par la Commission européenne comme offrant un niveau de protection adéquat (la décision d'adéquation de la Commission validant le Privacy Shield a été invalidée par la Cour de Justice de l'Union européenne [CJUE] le 16 juillet 2020 suite à l'arrêt dit « Schrems II[78] », le Privacy Shield ne constituant plus une garantie juridique suffisante pour transmettre des données personnelles de l'UE vers les USA).
Un nouveau bouclier *privacy* pourrait être adopté en 2023, cela n'est pas si évident selon la dernière **communication** du CEPD de février 2023. En tout état de cause, côté américain, **l'*Executive order*** du 7 octobre 2022 a grandement fait diminuer l'exposition au risque sur les données, simplifiant et sécurisant la régularisation des clauses contractuelles types et TIA associés.
Il s'agit donc pour l'avocat de peser le pour et le contre entre le niveau de sécurité et les moyens de protection objectivement avancés offerts par les géants américains du secteur et les spécificités liées à leur législation d'origine.

En tout état de cause, pour tout transfert qui n'est pas à destination d'un pays bénéficiant d'une décision d'adéquation, il faut procéder à l'évaluation du niveau de protection dont bénéficieront les données transférées en fonction des législations applicables dans le pays des destinataires de ces transferts (TIA, « Transfert Impact Assessment »).

76. https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre5#Article49.
77. Google, Apple, Meta, Amazon et Microsoft (ou GAFAM : Google, Apple, Facebook, Amazon et Microsoft).
78. CJUE, 16 juillet 2020, DPC c/ Facebook Ireland Ltd et M. Schrems, C-311/18.

Dans tous les cas de figure, l'analyse doit avoir pour objet de déterminer si les garanties contenues dans l'outil d'encadrement du transfert (CCT, BCR, etc.) peuvent être respectées dans la pratique ou si le cadre juridique de destination du transfert a pour effet de diminuer ou d'écarter l'application de ces garanties. La législation applicable en matière de renseignement et d'accès des autorités publiques compétentes doit faire l'objet d'un examen particulier, afin de déterminer si elle s'oppose à l'application des garanties prévues dans l'outil de transfert. Il peut également être nécessaire d'examiner d'autres législations sectorielles applicables aux spécificités de chaque transfert envisagé, par exemple le cadre juridique relatif aux données de santé, aux données financières, aux données relatives aux ressources humaines, etc. Dans le cas où la législation du pays tiers aboutit à écarter entièrement ou partiellement les garanties qui figurent dans l'outil de transfert, des mesures supplémentaires doivent être mises en place.

Le cas échéant, si les garanties ne sont pas suffisantes, la décision pourra être prise de changer de prestataire.

FICHE N° 11
LA GESTION DU DROIT D'ACCÈS AUX DONNÉES DES PERSONNES CONCERNÉES

Le droit d'accès aux données est le principe par lequel toute personne peut demander à un organisme, privé ou public, si ce dernier détient des données sur elle et, dans l'affirmative, de lui communiquer ses informations personnelles sous une forme compréhensible et claire (article 12 du RGPD) accompagnée d'informations concernant les traitements des données en question (article 15 du RGPD).

Ce droit permet aussi à la personne concernée de vérifier si des données la concernant sont traitées, et de quelle façon, et si le traitement mis en œuvre est licite. En clair, le demandeur doit être informé de la nature des informations personnelles que le responsable de traitement détient sur lui et doit pouvoir accéder facilement à ces informations.

Concrètement, un client, une personne dont les données sont traitées dans un dossier, un salarié ou collaborateur d'un cabinet d'avocats peut par exemple demander l'accès à son dossier et une communication des informations s'y trouvant. La demande portera ainsi sur les données détenues de manière générale et non sur des documents précis en particulier.

Les dispositions du RGPD, précisées dans le décret d'application n°2019-536 du 29 mai 2019 de la loi Informatique et libertés[79], prévoient notamment :

- concernant les **délais pour répondre à une demande :** le délai de réponse est d'un mois maximum à compter de la réception de la demande (article 12.3 du RGPD). 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. Typiquement, une demande d'accès d'une personne à l'ensemble de ses données traitées par l'avocat pourrait être considérée comme une demande complexe si ce dernier doit solliciter notamment tous ses sous-traitants.
- concernant les **frais de reproduction :** la réglementation prévoit un principe de gratuité pour les copies fournies dans le cadre d'une demande d'accès (article 12.5 du RGPD). 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.
- concernant les **modalités de la communication des données :** le RGPD prévoit un parallélisme des formes et précise que si la personne présente sa demande par voie électronique, les informations demandées sont communiquées sous une forme

79. Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement (article 12.3 du RGPD). Dans ce cadre, la communication des informations, surtout si elles revêtent un caractère sensible, devra être réalisée de manière suffisamment sécurisée (cf. *infra*) ;

- concernant **l'aide du sous-traitant au sens du RGPD (le cas échéant) :** le RGPD prévoit que le sous-traitant aide le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées le saisissent en vue d'exercer leurs droits (article 28.3.e du RGPD).

De manière générale, le fait que le sous-traitant apporte son appui au responsable de traitement pour les réponses aux demandes d'exercice des droits RGPD, tel que le droit d'accès, est mentionné dans les clauses de sous-traitance conclues entre les deux entités (voir sur ce sujet le modèle de clauses dispensé en annexe).

1. UN JUSTIFICATIF D'IDENTITÉ DU DEMANDEUR EST-IL OBLIGATOIRE POUR RÉPONDRE À UNE DEMANDE D'ACCÈS ?

Le droit d'accès est conditionné par une justification *a minima* de l'identité du demandeur, indispensable pour empêcher pléthores d'usurpations d'identité et la récupération de données personnelles par des tiers non autorisés.

Ainsi, pour exercer pleinement son droit d'accès, la personne doit justifier de son identité « par tout moyen » selon le RGPD et le décret d'application de la loi Informatique et libertés susmentionné, et l'avocat peut demander à cette personne qu'elle lui fournisse des éléments supplémentaires en cas de « doutes raisonnables » quant à son identité (le délai de réponse pourra alors être suspendu dans l'attente de la réception de ces éléments). Ainsi :

- une copie d'une pièce d'identité n'est pas obligatoirement à demander en toute situation,
- la plupart des demandes d'accès ayant lieu par courriel, il convient néanmoins de s'assurer de l'identité réelle de la personne cachée derrière la demande en ligne, ou du moins de l'interroger suffisamment sur ce point.

La difficulté sera pour l'avocat, en tant que responsable de traitement, de trouver un juste milieu entre ces deux règles. Il est ainsi recommandé de ne pas demander ce justificatif si un client, un salarié ou un collaborateur a formulé sa demande en passant par un espace authentifié, par exemple respectivement à partir de son compte sur le site Internet ou de la messagerie professionnelle mise à disposition par le cabinet (sauf cas particuliers), ou encore si un contact téléphonique suffisamment probant a eu lieu avec le client en amont ou en aval de la demande.

Une difficulté supplémentaire peut naitre du fait que les demandes peuvent être effectuée par un mandataire de la personne concernée. Le décret d'application de 2019 susvisé prévoit que *« Ces demandes peuvent être présentées par une personne spécialement mandatée à cet effet par le demandeur, après justification de son identité et de l'identité du mandant, de son mandat ainsi que de la durée et de l'objet précis de celui-ci. Le mandat doit également préciser si le mandataire peut être rendu destinataire de la réponse du responsable du traitement ou du sous-traitant.».*

NOTA : malgré toutes les précautions prises, il est impossible d'être assuré à 100 % que la personne à distance demandant l'accès à ses données est bien celle qu'elle prétend être (même si une copie de la carte d'identité portant sa signature présente de bonnes garanties).

Cette difficulté peut néanmoins être contrebalancée par le fait que, précédant la communication finale des informations, des mesures de sécurisation supplémentaires auront pu être mises en place pour faire diminuer au maximum les risques (cf. *infra*).

2. QUELLE FORME DOIT PRENDRE LA RÉPONSE À UNE DEMANDE D'EXERCICE DU DROIT D'ACCÈS ?

L'article 15.1 du RGPD énonce que l'avocat responsable de traitement, outre le fait qu'une personne puisse lui demander l'accès à ses informations, doit fournir à la personne concernée, si ses données sont bien traitées par lui, des informations supplémentaires concernant les traitements de données, et parmi elles :

- les finalités du traitement,
- les catégories de données à caractère personnel concernées,
- les destinataires ou catégories de destinataires[80] auxquels les données à caractère personnel ont été ou seront communiquées,
- la durée de conservation lorsque cela a été clairement défini par l'avocat, ou les critères utilisés pour déterminer cette durée,
- l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement,
- le droit d'introduire une réclamation auprès d'une autorité de contrôle,
- lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source,
- l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée,
- lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale, la personne concernée a le droit d'être informée des garanties appropriées, en vertu de l'article 46, en ce qui concerne ce transfert.

En outre, le responsable du traitement doit naturellement fournir une copie des documents et des données (voir ci-après).

80. L'avocat devra, si la personne en fait la demande, lui fournir la liste détaillée des destinataires (« spécifiques »), c'est-à-dire pas uniquement par exemple une mention « sous-traitant » concernant un prestataire mais la dénomination sociale précise de ce prestataire (**CJUE, 12 janvier 2023, C 154/21**).

3. DOIS-JE PRENDRE DES MESURES PARTICULIÈRES AU MOMENT DE COMMUNIQUER LES DONNÉES, NOTAMMENT PAR VOIE NUMÉRIQUE ?

Pour pallier le doute qui subsiste, sauf cas particuliers, sur l'identité d'une personne demandant l'exercice du droit d'accès à ses données, surtout par voie dématérialisée, il est fortement conseillé d'encadrer la communication des informations personnelles en sécurisant de manière optimale l'envoi ou le transfert, d'autant plus s'il s'agit d'un client dont les données traitées par l'avocat sont hautement personnelles voire sensibles (voir le point 1 de la partie I). En effet, une ou plusieurs pièce(s) jointe(s) transmise(s) par e-mail en clair, constituant les données fournies au titre du droit d'accès, ne semblent pas offrir par exemple toutes les garanties suffisantes de sécurité respectant les énonciations de l'article 32 du RGPD (voir le point 3.4 de la partie I).

Ainsi, les données devraient *a minima* être chiffrées et protégées par un mot de passe à forte entropie (voir la fiche n°6 « Les bonnes pratiques en termes de sécurité des données ») à l'aide d'un logiciel *open source* de cryptage et/ou de compression, le mot de passe devant être communiqué à la personne concernée par un canal différent (et connu de l'avocat si la demande provient d'un client actuel ou ancien). Le fichier généré pourra ensuite être déposé sur un cloud privé de confiance avec un lien de téléchargement unique et pourquoi pas le rajout d'un mot de passe robuste pour le téléchargement.

Les données pourraient aussi être copiées sur une clé USB n'ayant jamais servi, utilisée pour cette seule occasion, cette clé pouvant être :

- remise en main propre au requérant si cela est possible ;
- transmise par voie postale avec toutes les précautions nécessaires à ce type de transmission (notamment par le biais d'un envoi recommandé avec accusé de réception), les données devant avoir été préalablement chiffrées tandis que le code de déchiffrement aura été communiqué dans un courrier postal distinct du premier ou *via* un autre canal de communication si cela est possible.

4. JUSQU'OÙ PEUT ALLER LA RÉPONSE À UNE DEMANDE D'ACCÈS ?

Sur le principe que la demande d'accès concerne les données et non les documents, la question de la communication des e-mails échangés avec le demandeur se pose, tout comme celle des informations relatives aux connexions de ce dernier *via* des plateformes ou espaces en ligne (logs de connexion) :

- concernant les données contenues dans les mails : les informations identifiantes dans les mails sont théoriquement communicables au titre du droit d'accès. Il conviendra donc de communiquer les mails concernant la personne en respect du droit des tiers et des principes du secret des correspondances et du secret professionnel ;
- concernant les données contenues dans les logs de connexion : les traces informatiques laissées par les clients, collaborateurs et salariés du cabinet dans les différents logiciels, applications et systèmes d'exploitation sont dans la théorie communicables si elles ne sont pas totalement anonymisées. Néanmoins, la

fourniture de certaines de ces données pourrait divulguer des informations sur les systèmes de défense numérique du cabinet et compromettre la sécurisation globale des données qui s'y trouvent. Il est ainsi conseillé de ne fournir que les logs de connexion ne présentant aucun risque, après avis et conseils des sous-traitants en la matière.

5. EST-IL POSSIBLE DE NE PAS RÉPONDRE À UNE DEMANDE D'ACCÈS ?

La réponse dans les délais impartis à une demande d'accès aux données est prise au sérieux par la Cnil et une éventuelle plainte pour défaut de réponse du responsable de traitement par la personne concernée pourrait entraîner des conséquences néfastes pour l'avocat. Néanmoins, il existe des cas où des données ne pourront être communiquées à la personne en demande :

- le cabinet ne traite aucune donnée à caractère personnel concernant la personne à l'origine de la demande de droit d'accès,
- les données ont été totalement anonymisées de sorte qu'il serait impossible de remonter directement aux données de la personne à l'origine de la demande de droit d'accès,
- les données ne sont plus ou pas conservées/ont été effacées conformément au principe de limitation de la durée de conservation (voir le point 3.1.3 de la partie I ainsi que la fiche n°2 « La gestion des archives »),
- la demande est manifestement infondée ou excessive notamment en raison de son caractère répétitif (demandes multiples et rapprochées).

NOTA : le fait qu'une personne demande à nouveau la communication de données auxquelles elle a déjà eu accès ne doit pas être considéré systématiquement comme une demande excessive, le caractère répétitif étant alors apprécié au cas par cas par le responsable de traitement.

Enfin, l'avocat doit bien vérifier lors de sa réponse qu'il ne permet l'accès aux seules données dont la communication ne porte pas une atteinte disproportionnée aux droits d'autrui. Ainsi, les droits des tiers (secret des affaires et à la propriété intellectuelle, droit à la vie privée, secret des correspondances, données couvertes par le secret professionnel, etc.) vont venir restreindre l'éventail des données rendues accessibles ou communicables.

Si l'avocat ne donnait pas suite à une demande, il doit motiver sa décision et informer le demandeur des voies et délais de recours pour contester ladite décision.

6. UN AVOCAT DOIT-IL FAIRE DROIT À UNE DEMANDE D'ACCÈS FORMULÉE PAR LA PARTIE ADVERSE OU UNE PERSONNE CONCERNÉE PAR LE DOSSIER D'UN CLIENT POUR DES DONNÉES QUI LA CONCERNENT ?

L'avocat étant un auxiliaire de justice, en vertu de l'article 3 de la loi du 31 décembre 1971[81], il participe de ce fait, dans son activité juridictionnelle, à la mission de service public de la Justice. De surcroît, pour son activité judiciaire, les traitements des données à caractère personnel opérés par l'avocat le sont, notamment, sur la base légale de l'exécution d'une mission d'intérêt public (article 6-1-e du RGPD), qui est d'assurer l'accès au droit et à la justice de toute personne.

Par ailleurs, la profession d'avocat étant une profession réglementée, l'avocat devra également respecter des règles déontologiques et professionnelles propres, notamment le respect du secret professionnel mais également l'obligation de diligences dont son client est créancier et la sauvegarde des droits de ce dernier.

Or, dans le cadre d'une demande d'accès aux données traitées par l'avocat par la partie adverse, celui-ci risque de divulguer des informations couvertes par le secret professionnel. Ainsi, une communication des données mettrait en péril ses obligations de diligences et de défense des intérêts de son client car ceci impliquerait de dévoiler la stratégie de défense mise en place au bénéfice de son client.

Dans la plupart des cas, l'avocat se trouvera dans l'impossibilité de commenter l'existence même de la relation d'affaire avec le client ou concernant un dossier qui puisse contenir les données personnelles de la personne à l'origine de la demande.

C'est pourquoi l'avocat ne peut faire droit à une demande d'accès faite par la partie adverse ou une personne concernée par le dossier d'un client (ni même une demande d'effacement des données).

À FAIRE	
Rédiger en amont une procédure interne relative à l'exercice du droit d'accès	☐
Bien respecter les délais légaux de réponse, par défaut d'un mois **à la suite de** la demande	☐
Si activation de la prorogation du délai maximum de deux mois supplémentaires, ne pas oublier d'informer la personne concernée de cette prorogation avant la fin du délai initial d'un mois	☐
Sécuriser la communication des données personnelles et lesdites données en elles-mêmes si transmission par voie dématérialisée	☐
Ne pas porter atteinte au droit des tiers dans la réponse fournie à la personne en demande	☐
Ne pas porter atteinte au secret professionnel si la demande d'accès émane de la partie adverse	☐

Sur ce sujet, la Cnil a publié un article de portée générale sur son site Internet intitulé « Professionnels : comment répondre à une demande de droit d'accès ».

81. https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006902768

FICHE N° 12
LES POUVOIRS DE CONTRÔLE DE LA CNIL

Les avocats responsables de traitement peuvent faire l'objet de sanctions administratives importantes en cas de méconnaissance des dispositions du RGPD. Dans un tel cadre, la formation restreinte de l'autorité nationale de contrôle (la Cnil) peut notamment, après une procédure contradictoire :

- infliger une amende administrative ;
- prononcer un avertissement ou un rappel à l'ordre ;
- limiter temporairement ou définitivement un traitement ;
- suspendre les flux de données ;
- prononcer une injonction de se mettre en conformité (avec astreinte possible).

NOTA : la Cnil peut aussi mettre en demeure un cabinet de se mettre en conformité aux obligations de protection des données. Il s'agit d'une injonction du Président de la Cnil intervenant après une plainte ou un contrôle de l'autorité qui n'est pas à proprement parler une sanction. La mise en demeure peut être rendue publique et le nom du cabinet également.

La Cnil peut également retirer une certification délivrée à une entreprise ou ordonner à l'organisme de certification de retirer sa certification.

S'agissant des amendes financières 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.

Enfin, il existe désormais une procédure de sanction simplifiée pour les dossiers peu complexes ou de faible gravité (cf. *infra*).

1. LES SANCTIONS PRONONCÉES SONT-ELLES SYSTÉMATIQUEMENT RENDUES PUBLIQUES ?

La Cnil, lorsqu'elle prononce une amende ou un avertissement, à l'encontre d'un responsable de traitement, fait le choix de dévoiler ou non l'identité de l'organisme sanctionné lorsque la décision est rendue publique ; l'affichage du nom du sanctionné n'est ainsi pas automatique et dépend du bon vouloir de la Commission, laquelle doit justifier cet affichage. Ainsi les avocats, en cas de sanction de l'autorité de contrôle, prennent le risque que leur nom ou celui de leur cabinet soit révélé au grand jour en cas de manquement aux obligations « Informatique et Libertés » et au RGPD.

NOTA : au-delà de la sanction financière potentielle, le déficit « d'image » semble tout aussi important, un avertissement public pouvant porter atteinte à la réputation du cabinet.

2. QUELS SONT LES DIFFÉRENTS TYPES DE CONTRÔLE OPÉRÉS PAR LA CNIL ?

Le contrôle le plus emblématique de la Cnil est sans conteste le contrôle sur place : des agents de l'autorité nationale, généralement au nombre de deux (un juriste et un ingénieur), se rendent au sein des locaux d'un responsable de traitement ou d'un sous-traitant afin de mener des investigations portant sur des traitements de données personnelles.

Mais les récentes crises sanitaires ont obligé la Cnil à s'adapter et ont notamment permis la mise en lumière d'autres moyens de contrôle à sa disposition :

- Le contrôle en ligne : sans quitter leurs bureaux, les agents de la Cnil vérifient à distance par exemple les sites Internet, applications mobiles, serveurs, etc. auxquels ils peuvent avoir accès librement. L'examen en ligne peut d'ailleurs prendre en compte les éventuelles données rendues accessibles par inadvertance par les responsables de traitement et sous-traitant et dont l'accès libre peut constituer une violation de données. Le contrôle en ligne est autorisé pour la Cnil depuis la loi Hamon de 2014[82].
- Le contrôle sur pièces : les agents de la Cnil demandent des informations relatives à des traitements mis en œuvre par un responsable de traitement ou un sous-traitant, informations pouvant être transmises par courrier et accompagnées de toute la documentation utile permettant d'évaluer la conformité de ces traitements.
- L'audition sur convocation : les agents de la Cnil demandent des informations directement aux organismes visés dont les représentants sont sommés de se présenter au sein des locaux de la Commission pour répondre à toutes leurs questions.

82. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028738036

3. COMMENT SE DÉROULE LA NOUVELLE PROCÉDURE DE SANCTION SIMPLIFIÉE DE LA CNIL ?

Pour répondre aux plaintes de plus en plus nombreuses reçues ces dernières années, l'autorité nationale de contrôle a modifié ses procédures répressives en 2022 en créant notamment une nouvelle procédure simplifiée de sanction pour des dossiers ne présentant pas de difficulté particulière, mais pouvant néanmoins justifier une sanction.

Le renvoi d'un dossier vers la procédure simplifiée reste un choix du Président de la Cnil et suit les mêmes étapes que la procédure de sanction ordinaire mais avec des modalités de mise en œuvre allégées (exemple : pas de séance publique sauf si l'organisme demande à être entendu).

Les sanctions maximales pouvant être prononcées dans ce cadre peuvent atteindre un montant de 20 000 € en amende, une injonction avec astreinte plafonnée à 100 € par jour de retard et un rappel à l'ordre. Ces sanctions ne sont jamais rendues publiques.

4. COMMENT SE DÉROULE UN CONTRÔLE SUR PLACE DE LA CNIL ?

Il est tout d'abord possible que la Cnil, dans le cadre d'un contrôle sur place, informe préalablement un cabinet d'avocats que celui-ci va être contrôlé. Cette information n'est évidemment pas une obligation, le contrôle « surprise » évitant *a minima* que les avocats puissent se « préparer » au contrôle et tentent par exemple de régler plusieurs problèmes de conformité dans le temps imparti (purge des données devant l'être, mise en place de registres non établis, etc.).

Les agents de la Cnil doivent obligatoirement, à leur arrivée, décliner leur identité (carte professionnelle) et rappeler au cabinet contrôlé la possibilité pour ce dernier de s'opposer au contrôle.

Les agents de la Commission, une fois présents dans les locaux du cabinet, peuvent :

- prendre copie de toute information (copie des contrats, de dossiers papier, extraction de bases de données) et/ou demander communication de tous documents permettant d'apprécier les conditions dans lesquelles sont mis en œuvre les traitements de données personnelles,
- accéder à tous les espaces, physiques ou numériques, contenant des données personnelles,
- interroger toute personne maniant des données personnelles ou susceptible de détenir des informations utiles pour apprécier la conformité des traitements de données personnelles.

L'avocat peut opposer aux contrôleurs de la Cnil le secret professionnel concernant les informations couvertes par ce dernier, par exemple les correspondances avec ses clients. La mention de l'opposition, son fondement textuel et la nature des données couvertes seront alors inscrits sur le procès-verbal établi par les agents de la Cnil.

À l'inverse, l'avocat prend un risque en cas d'invocation injustifiée du secret professionnel pour ne pas laisser les contrôleurs de la Commission accéder aux données, constituant un délit d'entrave[83] passible d'une peine d'un an d'emprisonnement et de 15 000 € d'amende.

5. EST-IL UTILE DE SENSIBILISER SES COLLABORATEURS ET SON PERSONNEL À UN ÉVENTUEL CONTRÔLE ?

L'ensemble des membres d'un cabinet doit être préparé en amont à un potentiel contrôle de la Cnil et sensibilisé en ce sens. En fonction de la situation, le personnel d'accueil, les collaborateurs et/ou les associés d'un cabinet se retrouveront en première ligne en cas de contrôle sur place de l'autorité nationale et devront adopter les bons réflexes pour réagir promptement à cette situation inédite :

- ne pas hésiter à demander aux contrôleurs leur carte professionnelle si ceux-ci ne la présentaient pas spontanément (ce qui n'arrive théoriquement jamais),
- ne pas hésiter à vérifier directement auprès de la Cnil (par téléphone) qu'un contrôle a bien été diligenté au sein du cabinet : ceci permet de démasquer des personnes malintentionnées munies de faux justificatifs et venues pour accéder aux informations du cabinet,
- prévenir immédiatement le délégué à la protection des données (voir le point 4 de la partie II) s'il existe ou toute personne désignée comme référente sur les questions de protection des données personnelles et lui demander de se présenter en urgence (même si la fonction est externalisée),
- envoyer dans un même temps un e-mail préformaté à l'ensemble des collaborateurs et du personnel (si ceci est pertinent en fonction de la taille du cabinet) pour les informer de la tenue du contrôle,
- inviter les contrôleurs à patienter le temps que le DPD ou un référent du cabinet n'arrive, bien que rien n'empêche un agent de la Cnil d'investiguer dès son entrée dans les locaux.

83. Article 226-22-2 du Code pénal

ANNEXES PRATIQUES

- Registre type des activités de traitement en tant que responsable de traitement
- Documentation relative aux violations de données (sous la forme d'un registre)
- Référentiel de durées de conservation pour les données et documents du cabinet
- Check-list de conformité
- Modèles de mentions d'information
- Registre des demandes d'exercice des droits relatifs à la protection des données
- Réponses types à des demandes d'exercice de droit
- Formulaire de demande d'exercice de droit
- Clauses de sous-traitance RGPD
- Registre des sous-traitants du cabinet
- Méthodologie pour l'élaboration d'une charte informatique du cabinet

POUR ALLER PLUS LOIN

- **Textes utiles en vigueur :**
  - Règlement général sur la protection des données
  - Loi Informatique et libertés
  - Article L. 34-5 du Code des postes et des communications électroniques
  - Article 66-5 de la loi du 31 décembre 1971
  - Article 226-13 du Code pénal
- **Lignes directrices du CEPD (ex-G29) :** https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_fr
- **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
- **Documents d'information et ressources de la Cnil :**
  - Se préparer en 6 étapes
  - Guide de la sécurité des données personnelles
  - Thématique sécurité sur le site Internet de la Cnil
  - Guide sur les durées de conservation des données
  - Référentiel relatif aux traitements de données de ressources humaines (RH)
  - Guide pour le recrutement (RH)
  - Guide relatif aux « tiers autorisés »
  - Recueil des procédures « tiers autorisés »
  - Guide sur le métier de délégué à la protection des données (DPO)
  - Guide du développeur (pour tout prestataire concerné ou équipe de développement informatique)
  - L'Atelier RGPD (MOOC)
- **Commission européenne :**
  - Outil en ligne, comprenant des fiches pratiques, questions/réponses et 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

LISTE DES PERSONNES AYANT CONTRIBUÉ À L'ÉLABORATION DE LA DEUXIÈME ÉDITION DU GUIDE

- **Pour le Barreau de Paris :**
  - Nadine MOKDAD, déléguée à la protection des données
- **Pour le Conseil national des barreaux :**
  - Axelle DESHAIRES, juriste numérique
  - Johan ESPINASSE, juriste numérique
  - Guillaume LHUILLIER, délégué à la protection des données
- **Pour la Conférence des Bâtonniers :**
  - Laurent CARON, avocat au Barreau de Paris, délégué à la protection des données

Les rédacteurs remercient chaleureusement les relecteurs de cette deuxième édition, et parmi eux :

- Philippe BARON, président de la commission numérique du Conseil national des barreaux,
- Isabelle GRENIER, membre de la commission numérique du Conseil national des barreaux,
- Stéphanie FABER, avocate au Barreau de Paris,
- Valérie HAYEK, avocate au Barreau de Paris, experte en Droit des technologies de l'information au CCBE, Membre de la Commission Numérique - RGPD et Relations Internationales du Barreau de Paris,
- Éric LE QUELLENEC, avocat au Barreau de Paris,
- le service des délégués à la protection des données et de l'accompagnement de la Commission nationale de l'Informatique et des Libertés.

CONSEIL NATIONAL DES BARREAUX
LES AVOCATS

2e édition | Mai 2023
Établissement 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

Ce document est à destination exclusive des avocats