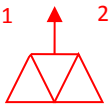

CHIFFRE & DROIT

COMPETENCES ET CONSEILS

PRESENTATION DU RGPD
LA PROTECTION DES DONNEES PERSONNELLES

Sarah ALLOUCHE, Avocat à la Cour

Sylvain REINGEWIRTZ, Expert-Comptable

Réunion du 21 juin 2018

PARTIE 1 – PRESENTATION DU RGPD

I – L'ADOPTION DU RGPD ET SON CHAMP D'APPLICATION :

A. Le RGPD et les raisons d'une nouvelle règlementation :

Le Règlement Général sur la Protection des Données (RGPD) est la nouvelle règlementation relative à la gestion, la collecte et le traitement des données personnelles issue du Règlement UE 2016/679 relatif à la protection des données.

Le RGPD est entré en vigueur le 24 mai 2016.
Depuis cette date, les autorités nationales ne peuvent plus adopter des dispositions qui lui soient contraires.

Il est applicable depuis le 25 mai 2018 et produit immédiatement, de manière simultanée et uniforme, ses effets dans les ordres juridiques nationaux.

Il permet aux droits nationaux pour certains domaines de « préciser » le Règlement, de prévoir des « règles spécifiques » ou de déroger au règlement (RGPD art. 85 à 91).

Forcément, la France n'envisage pas de renoncer à sa législation et notamment à la Loi 78-17 du 6 janvier 1978 dite « Informatique et Libertés » et la loi du 6 août 2004 qui avait transposé une Directive 95-64 du 24 octobre 1995 qui souhaitait harmoniser les législations des Etats Membres sur la protection des données personnelles.

Le RGPD va donc constituer une occasion de refondre le droit national en y apportant 3 séries de modifications :

- Supprimer les articles dont la substance est reprise par le RGPD ou qui ne peuvent pas coexister avec lui ;
- Redéfinir les pouvoirs de la Cnil et les procédures liées à l'exercice de ses attributions ;
- Fixer les règles applicables dans les hypothèses où les autorités nationales conservent une marge d'appréciation qui leur permet d'ajouter des éléments supplémentaires au règlement ou encore de s'écarter de celui-ci.

Certaines dispositions du Code pénal vont également être modifiées et adaptées au RGPD, notamment les articles 226-16 et suivants régissant les infractions aux dispositions de la Loi de 1978.

Un projet de Loi du 14 mai 2018 est déjà en cours d'examen par le Parlement.

B. Le champ d'application du RGPD :

Comme tout texte de loi, le RGPD précise son champ d'application matériel et territorial.

1. Le champ d'application matériel :

Le RGPD, au même titre de la Loi « Informatique et Libertés » s'applique aux **traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données personnelles contenues ou appelées à figurer dans un fichier** (RGPD art. 2, 1).

Il s'applique également aux Responsables de traitement ou aux sous-traitants qui fournissent les moyens de traiter les données personnelles pour de tels traitements.

Ne sont pas concernés par le RGPD les traitements de données personnelles effectués :

- dans le cadre d'une activité qui ne relève pas du droit de l'Union ;
- par les Etats membres dans le cadre d'activités qui relèvent de la politique étrangère et de la sécurité commune de l'Union ;
- par une personne physique dans le cadre d'une activité strictement personnelle ou domestique, par exemple l'échange de correspondances, la tenue d'un carnet d'adresse, l'utilisation de réseaux sociaux et les activités en ligne;
- par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite dans ce domaine ou d'exécution de sanctions pénales, cette exclusion s'étendant également à la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

2. Le champ d'application territorial :

Le RGPD s'applique à titre principal aux traitements de données personnelles **lorsque le Responsable de traitement ou le sous-traitant de ce dernier, est établi sur le territoire de l'Union, sans considération du lieu où le traitement est effectué**.

Le RGPD est **également applicable** aux traitements de données personnelles dans lesquels le Responsable de traitement ou le sous-traitant ne sont pas établis dans l'Unions **mais pour lesquels les personnes concernées sont des résidents européens « ciblés » en vue d'une offre de biens ou de services**.

Entrent également dans le champ d'application territorial du RGPD les traitements liés « au suivi » sur Internet d'une personne concernée dans le but de réaliser un profilage.

3. Qui est concerné par le RGPD ?

Le RGPD s'applique à **toute organisation publique ou privée qui traite des données personnelles pour son compte ou non dès lors que :**

- **elle est établie sur le territoire de l'Union européenne,**
- **son activité cible directement des résidents européens.**

Par exemple, une société établie en France, qui exporte l'ensemble de ses produits en dehors de l'Union européenne doit respecter le RPGD.
De même, une société établie en dehors de l'Union européenne proposant un site de e-commerce en français livrant des produits en France doit respecter le RGPD.

Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organismes.

A ce titre, les cabinets d'avocats et d'experts-comptables, dès lors qu'ils collectent et traitent des données personnelles, sont concernés par le RGPD et doivent se mettre en conformité avec les règles qu'il édicte.

II – LE TRAITEMENT DES DONNEES A CARACTERE PERSONNEL ET LES DROITS DE LA PERSONNE CONCERNEE :

A. Règles relatives au traitement de données personnelles :

1. Qu'est-ce qu'une donnée à caractère personnel ?

Constitue une **donnée à caractère personnel** « *toute information se rapportant à une personne physique identifiée ou identifiable* », laquelle est dénommée « personne concernée ».

Est considérée comme « identifiable », une personne physique qui peut être identifiée :

- **Directement** : prénom, nom, adresse e-mail,
- **Indirectement** : par référence à un identifiant, un numéro client, un numéro de téléphone, un numéro d'immatriculation, une donnée biométrique, plusieurs éléments spécifiques à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi par la voix ou l'image,
- **A partir d'une seule donnée** : numéro de sécurité sociale, ADN ;
- **A partir du croisement d'ensemble de données** : par exemple une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association.

2. Qu'est-ce qu'un traitement de données à caractère personnel ?

Le **traitement de données personnelles** est « *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* ».

Exemples de traitement : tenue d'un fichier de ses clients, collecte des coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, etc...

Par contre, n'est pas considéré comme un traitement de données personnelles un fichier ne contenant que des coordonnées d'entreprises (par exemple entreprise "Compagnie A" avec son adresse postale, le numéro de téléphone du standard et un email de contact générique "compagnieA@email.fr").

Un traitement de données personnelles **n'est pas nécessairement informatisé** : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Un traitement de données doit avoir un objectif, **une finalité**, c'est-à-dire, qu'il n'est pas possible de collecter ou traiter des données personnelles simplement au cas où elles seraient utiles un jour.

A chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de l'activité professionnelle considérée.

Par exemple, vous collectez sur vos clients de nombreuses informations lorsque vous effectuez une prestation dans son intérêt ou éditez une facture. Toutes ces opérations sur ces données constituent votre traitement de données personnelles ayant pour objectif la gestion de votre clientèle.

3. Les principes généraux relatifs à la collecte et au traitement des données personnelles

Le RGPD pose **6 principes généraux relatifs à la collecte et au traitement des données personnelles**, lesquels coïncident largement avec ceux qui se dégagent de la loi de 1978 :

- **le principe de limitation des finalités** : les données personnelles doivent être collectées à des fins déterminées, explicites et légitimes, sans qu'elles puissent faire ultérieurement l'objet d'un traitement incompatible avec ces finalités. Les personnes concernées doivent ainsi être informées de la finalité du traitement de leurs données personnelles ;
- **Le principe de « licéité, loyauté et transparence »** : les données personnelles doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée. Le traitement des données personnelles doit avoir **une finalité autorisée**. Les personnes

concernées doivent être informées de l'existence de ce traitement, lequel doit correspondre à la description qui en est faite ;

- **Le principe de minimisation des données** : les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du traitement. Les données collectées doivent être **strictement nécessaires au traitement**. Il faut veiller à ne pas collecter ou transmettre plus de données personnelles que celles nécessaires.
- **Le principe d'exactitude** : les données personnelles doivent exactes et, si nécessaires, tenues à jour. Il est recommandé de mettre en place une procédure pour que les données soient toujours à jour. Ce principe permet notamment l'exercice par la personne concernée de son droit de rectification ;
- **Le principe de limitation de la conservation** : les données personnelles doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle qui est nécessaire au regard des finalités du traitement. Quand les données ne sont plus nécessaires au traitement, elles doivent être supprimées ou anonymisées ;
- **Le principe d'intégrité et de confidentialité** : les données personnelles doivent être traitées de façon à garantir une sécurité appropriée, en assurant notamment leur protection contre les traitements non autorisés ou illicites, ainsi que contre la perte, la destruction ou les dégâts d'origine accidentelle. Le responsable du traitement s'expose ainsi à des sanctions en cas de violation des données personnelles.

4. La licéité d'un traitement de données personnelles :

a) Les six bases légales d'un traitement

Le RPGD pose 6 bases légales pour la licéité d'un traitement de données personnelles.

1 – Le **consentement de la personne concernée :** il s'agit d'une manifestation de volonté « **libre, spécifique, éclairée et univoque** ».
Il implique de la part de la personne concernée une « déclaration » ou un « acte positif clair », manifestation que l'on retrouve dans la pratique de l'« opt-in actif » (case à cocher).

Il existe plusieurs garanties du principe du consentement :

- Le Responsable de traitement doit pouvoir **démontrer que le consentement a été effectivement donné** ;
- Si le consentement porte sur plusieurs questions, la demande de « **consentement multiple** » doit être présentée sous une forme compréhensible, aisément accessible et formulée en des termes clairs et simples ;
- La personne concernée a le **droit de retirer son consentement à tout moment**. Le retrait du consentement ne remet pas en cause la licéité du traitement fondé sur le consentement initial.

2 – A défaut de consentement, le traitement de données personnelles est licite s'il est nécessaire :

- à l'exécution d'un contrat auquel est partie la personne concernée ;

- au respect d'une obligation légale incombant au responsable du traitement ;
- à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- à l'exécution d'une mission d'intérêt public, ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ;
- aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que les intérêts et droits fondamentaux de la personne concernée ne prévalent sur les intérêts du responsable du traitement.

b) Les dispositions particulières applicables aux enfants :

Le traitement n'est licite que si l'enfant est âgé d'au moins 16 ans.

Si l'enfant est âgé de moins de 16 ans, le consentement doit être donné par le titulaire de la responsabilité parentale.

Le RGPD permet aux Etats Membres de réduire à 13 ans cette limite d'âge.

Mais le RGPD ne peut pas être considéré comme créant une dérogation au droit général des contrats des Etats Membres, et, notamment, aux règles concernant la validité, la formation ou les effets d'un contrat à l'égard d'un enfant.

c) Le traitement des données sensibles :

Le RGPD interdit par principe le traitement de certaines données personnelles dites « données sensibles », à savoir : toutes les données qui révèlent

- l'origine raciale ou ethnique des personnes,
- leurs opinions politiques,
- leurs convictions religieuses ou philosophiques, leur appartenance syndicale,
- leur santé,
- leur vie
- leur orientation sexuelles,
- les « données génétiques ;
- les « données biométriques.

Mais il existe de nombreuses dérogations au principe d'interdiction de traitement des « données sensibles » :

- **la personne concernée a donné son consentement explicite** au traitement de ces données, pour une ou plusieurs finalités spécifiques, sauf si le droit de l'Union ou le droit national prévoit que l'interdiction ne peut pas être levée par la personne concernée ;
- **le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique**, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

- **le traitement porte sur des données personnelles qui sont manifestement rendues publiques par la personne concernée** ;
- **le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice** ou encore chaque fois des juridictions « agissent dans le cadre de leurs fonctions juridictionnelles » ;
- **le traitement est nécessaire aux fins de médecine** préventive ou de médecine du travail, de diagnostics médicaux, de « prise en charge sanitaire et sociale », ou encore de gestion de systèmes de soins et de protection sociale ;
- **les traitements nécessaires à l'exécution des obligations et à l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale** ;

d) Le traitement des données relatives aux condamnations pénales et infractions :

Comme le fait la législation nationale, le RGPD soumet à des dispositions particulières ou à des mesures de sécurité le traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions.

Ce traitement ne peut être effectué que :
- sous le contrôle de l'autorité publique ;
- ou, à condition d'être autorisé par le droit de l'Union ou celui d'un Etat membre, lequel doit prévoir des garanties appropriées pour les droits des personnes concernées.

De plus, tout registre complet de condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique.

Une exception à cette interdiction de principe concerne directement les avocats qui peuvent dans le cadre de leur mission de défense de leurs clients être amenés à collecter et traiter ces données relatives aux condamnations pénales et infractions.

B. Les droits des personnes concernées :

Une personne concernée est « *une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » (article 4§1 du RGPD).

Le RGPD renforce les droits des personnes sur leurs données à caractère personnel.

La personne concernée dispose des droits suivants :

- ✓ **Le droit à l'information** :

L'article 13 du RGPD prévoit que le responsable du traitement doit, **de sa propre initiative**, fournir à la personne concernée les informations suivantes :

- Les coordonnées du responsable du traitement et, le cas échéant, celles du représentant du responsable du traitement,
- Le cas échéant, les coordonnées du délégué à la protection des données,
- Les finalités du traitement auquel sont destinées les données à caractère personnel,
- La base juridique du traitement,
- Les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers lorsque ces intérêts légitimes sont la condition de la licéité du traitement,
- Le fait que le responsable du 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 dru 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 de l'autorité de contrôle,
- Les 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 concernées.

Ces informations, lorsqu'elles sont collectées directement, doivent être communiquées à la personne concernée au moment où les données en question sont obtenues **sauf si la personne concernée dispose déjà des informations visées**.

Lorsque la collecte est **indirecte**, les informations doivent être transmises à la personne concernée :

- dans un « délai raisonnable », ne dépassant pas un mois, après l'obtention des données ;
- au moment de la première communication, si les données doivent être utilisées aux fins de communication avec la personne concernée ;
- au plus tard lorsque ces données sont communiquées pour la première fois, s'il est envisagé de communiquer les données personnelles à un autre destinataire ; .
- à chaque fois que le responsable de traitement envisage d'effectuer un traitement ultérieur des données pour une finalité autre que celle pour laquelle les données personnelles ont été obtenues.

Mais il existe des dérogations à ce principe d'information de la personne concernée :

- Il s'agit de l'hypothèse où la personne concernée dispose déjà des informations dont le RGPD prescrit la transmission ;
- la fourniture des informations prévues par le RGPD se révèle impossible ou exigerait des efforts disproportionnés ;
- l'obtention ou la communication des informations sont expressément prévues par le droit de l'Union ou celui d'un Etat membre ;
- les données personnelles doivent rester confidentielles en vertu d'une obligation de secret professionnel.

L'article 14 du RGPD énumère quant à lui les informations à communiquer lorsque les données à caractère personnel ne sont pas directement collectées auprès de la personne concernée.

C'est notamment le cas lorsque, dans le cadre d'un dossier, le client transmet des informations sur la partie adverse à l'avocat.

L'article 14 du RGPD prévoit donc que la personne doit être informée des éléments prévus à l'article 13 du RGPD (ci-dessus) mais également ;

- les catégories des données personnelles collectées ;
- la source d'où proviennent les données à caractère personnel
- et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public.

Une telle information poserait une difficulté pour l'avocat puisque le respect de cette obligation impliquerait d'informer la partie adverse de la constitution du dossier par l'avocat et donc de mettre en péril les intérêts de son client.

Il sera ainsi possible dans cette hypothèse d'opposer l'exception à l'obligation d'information fondée sur le fait que les données personnelles doivent rester confidentielles en vertu d'une obligation de secret professionnel.

- ✓ <u>Le droit d'accès :</u>

Le droit d'accès est le droit, pour toute personne justifiant de son identité, d'interroger le responsable d'un fichier ou d'un traitement pour savoir s'il détient des informations sur elle.

Dans l'affirmative, elle a le droit d'accéder à ces données et de recevoir certaines informations, dont notamment :

- Les finalités du traitement ;
- Les catégories de données personnelles concernées ;
- Les destinataires ou catégories de destinataires ;
- L'existence d'une prise de décision automatisée et logique sous-jacente du traitement ;
- Les garanties entourant un transfert de données vers un pays tiers si ce dernier ne fait pas l'objet d'une décision d'adéquation,
- La durée de la conservation des données personnelles, ou, à défaut, critères utilisés pour déterminer cette durée ;
- Les autres droits ouverts à la personne concernée ;
- Le droit de réclamation auprès de l'autorité de contrôle ;
- La source des données si elles n'ont pas été directement auprès de la personne concernée.

Le Responsable de traitement <u>est tenu de fournir une copie des données personnelles</u> :

- **Sous un délai d'un mois maximum** à compter de la réception de la demande ; ce délai peut être prolongé de 2 mois « *compte tenu de la complexité et du nombre de demandes* » à condition d'en informer la personne concernée dans le délai d'un mois de la réception de la demande ;
- **Gratuitement** ; mais la copie sera payante (« frais raisonnables ») si la demande est manifestement infondée ou excessive ou en cas de copie supplémentaire ;
- **Par un format identique que celui par lequel la demande d'accès est formulée**. Si la personne présente sa demande par voie électronique, les informations demandées seront communiquées par une forme électronique d'usage courant à moins que la personne concernée ne demande qu'il en soit autrement (article 12.3).

- ✓ <u>Le droit de rectification :</u>

Selon l'article 16 du RGPD, « *la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais,* ***la rectification des données à caractère personnel la concernant qui sont inexactes****. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel* ***incomplètes soient complétées****, y compris en fournissant une déclaration complémentaire* ».

La personne concernée dispose du droit d'obtenir du responsable du traitement que celui-ci rectifie éventuellement les données faisant l'objet de ce traitement ou les complète selon la « déclaration complémentaire » fournie par la personne concernée.

- ✓ <u>Le droit d'effacement ou le droit à l'oubli :</u>

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

Cette disposition trouve sa source dans l'affaire Google Spain SL, Google Inc contre Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez, dans laquelle la Cour a jugé que les personnes physiques sont en droit (sous réserve de certaines conditions et garanties) de demander à un moteur de recherche de supprimer les liens renvoyant à des données à caractère personnel les concernant.

Il est cependant relatif et suppose que soit effectué **un contrôle de proportionnalité entre les intérêts de la personne concernée et ceux du responsable du traitement ou, le cas échéant, du public en général (droit à l'information ou intérêt historique)**.

Pour l'Avocat ou l'expert-comptable, l'effacement irréversible des données d'un client ne pourra être mis en œuvre avant l'expiration de la durée de la prescription de la responsabilité civile professionnelle.

Il est en effet important de noter que le droit à l'oubli ne prévaut pas évidemment pas sur certaines obligations d'archivage de données pendant des périodes déterminées, par exemple pour des raisons de conformité aux obligations fiscales ou de prescription.

Le droit à l'oubli permet d'obtenir du responsable du traitement l'effacement, « dans les meilleurs délais », de certaines données personnelles, lorsque l'une des conditions ci-après se trouve satisfaite :

- les données ne sont plus nécessaires au regard des finalités du traitement pour lesquelles elles ont été collectées ou traitées ;
- la personne concernée a retiré son consentement au traitement ;
- la personne concernée s'est opposée au traitement des données ;
- les données personnelles ont fait l'objet d'un traitement illicite ;
- les données doivent être effacées pour respecter une obligation légale prévue par le droit de l'Union ou celui de l'Etat membre auquel le responsable du traitement est soumis ;
- les données ont été collectées auprès d'enfants et qui demandent leur suppression, une fois devenus adultes.

Si les données à effacer ont été rendues publiques, le responsable du traitement doit alors, « *compte tenu des technologies disponibles et des coûts de mise en œuvre* », prendre des mesures « *raisonnables* » pour faire connaître aux autres responsables traitant ces données que la personne concernée a demandé qu'ils effacent tout lien avec elles ou encore toute copie ou reproduction de ces données.

Mais le droit à l'oubli connait de nombreuses exceptions et ne pourra pas être réalisé si le traitement est nécessaire :

- à l'exercice du droit à la liberté d'expression et d'information ;
- pour respecter une obligation légale prévue par le droit de l'Union ou celui de l'Etat membre auquel le responsable du traitement est soumis, ou encore pour exécuter une mission d'intérêt public, ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- pour des motifs d'intérêt public dans le domaine de la santé publique (par exemple le traitement de données sensibles et les des traitements nécessaires à la médecine préventive) ;
- à des fins archivistiques, dans l'intérêt public, à des fins de recherche scientifique ou historique, ou encore à des fins statistiques, dans la mesure où l'effacement des données risque de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement ;
- pour la constatation, l'exercice ou la défense de droits en justice.

✓ **Le droit à la limitation du traitement :**

La « limitation » du traitement est définie comme l'isolation, le marquage de données à caractère personnel enregistrées, en vue de limiter leur traitement futur ou actuel. La limitation du traitement constitue une sorte de « *séquestre numérique* ».

Le RGPD permet désormais à la personne concernée d'obtenir du responsable du traitement qu'il « limite » celui-ci.

Le Règlement autorise la personne concernée à revendiquer la limitation du traitement de données à caractère personnel dans 4 cas de figure :

- lorsqu'elle conteste l'exactitude d'une donnée, le temps que le responsable puisse contrôler celle-ci ;
- si le traitement est illicite et qu'elle s'oppose néanmoins à leur effacement, préférant une telle limitation ;
- lorsque la personne concernée en a besoin pour la constatation, l'exercice ou la défense de ses droits en justice même si le responsable du traitement n'en a plus besoin aux fins du traitement ;
- lorsque la personne concernée s'est opposée au traitement, le temps pour le responsable du traitement d'examiner le caractère fondé de la demande ou de vérifier si les intérêts légitimes qu'il poursuit peuvent faire échec à cette demande d'opposition.

En cas de limitation du traitement, les données concernées ne peuvent plus faire l'objet d'un quelconque traitement, **à l'exception de leur conservation, et sauf consentement de la personne**.
Les données faisant l'objet d'une limitation peuvent néanmoins encore être traitées :

- pour la constatation, l'exercice ou la défense de droits en justice,
- pour la protection des droits d'une autre personne morale ou physique,
- ou encore pour des motifs importants d'intérêt public dans l'Union ou l'État membre.

- ✓ **Le droit à la portabilité des données :**

Le RGPD institue un droit nouveau qui permet aux personnes concernées de recevoir les données qu'elles ont « fournies » au responsable du traitement afin qu'elles soient « transmises » à un autre responsable de traitement, même concurrent.

Le droit à la portabilité des données ne peut être exercé que :

- Par la personne concernée ;
- S'il ne porte pas atteinte aux droits et libertés d'autres personnes, ce qui inclut le respect des données à caractère personnel de tiers et le respect des données couvertes par un droit de propriété intellectuelle et/ou le secret des affaires.

Ce droit ne peut s'exercer qu'à **deux conditions** :

- le traitement est fondé sur le consentement de la personne concernée ou le traitement est nécessaire à l'exécution d'un contrat auquel est partie la personne concernée ;

et

- s'il est effectué à l'aide de procédés automatisés, ce qui exclut les données contenues dans des fichiers manuels.

Lorsque les deux conditions exposées ci-dessus sont satisfaites, la personne concernée doit recevoir les données en cause « *dans un format structuré, couramment utilisé et lisible par machine* », tout en ayant la possibilité de le transmettre à un autre responsable du traitement.

Mais le droit à la portabilité des données ne doit pas empêcher l'exercice ultérieur ou concomitant de ses autres droits par la personne concernée, notamment le droit à l'oubli.

Il ne signifie pas non plus que le responsable de traitement ne peut plus traiter les données ayant fait l'objet de ce droit : la suppression des données n'est pas automatique et leur durée de conservation n'est pas modifiée.

- ✓ **Le droit d'opposition :**

Sur ce point, les dispositions du RGPD diffèrent en partie de celles retenues par la loi de 1978.

Selon la législation nationale, **toute personne est en droit de s'opposer, pour des motifs légitimes, à ce que des données la concernant fassent l'objet d'un traitement**.

Selon le RGPD, le droit d'opposition s'exerce, à tout moment pour des raisons relatives à la « situation particulière » de la personne concernée.

Alors que la Loi « Informatique et Libertés vise « tous les traitements », le RGPD limite le droit d'opposition à deux types de traitements (dont le profilage) fondés sur une autre base légale que le consentement :

- lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.
- lorsque le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers.

Dès lors que le droit d'opposition est exercé, **le responsable du traitement est tenu de ne plus traiter les données personnelles en cause** sauf s'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

Le droit d'opposition porte également sur le traitement de données :

- à des fins de prospection commerciale et le profilage lié à cette prospection.
- à des fins de recherche scientifique ou historique, ou à des fins statistiques, sauf si le traitement est nécessaire à l'exécution d'une mission d'intérêt public.

Afin de permettre son exercice éventuel, le droit d'opposition doit être explicitement porté à la connaissance de la personne concernée (qui n'a pas consenti au traitement) **au plus tard au moment de la première communication** et doit être présenté clairement et séparément de toute autre information.

- ✓ **Les droits annexes :**

A ces droits s'ajoutent :

- **Le droit à la notification de la rectification, effacement ou limitation de leurs données** : le droit crée une obligation de notification à charge du responsable de traitement qui l'oblige à communiquer à chaque destinataire des données toute rectification, effacement ou limitation du traitement ;

- **Le droit de ne pas être soumis à une décision individuelle automatisée** : La personne concernée a le droit de ne pas être soumise à une décision résultant exclusivement d'un traitement automatisé produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire. Le profilage y est expressément inclus ;

- **Le droit à la communication d'une violation de données à caractère personnel** : Le **responsable** de traitement est obligé de notifier à la personne concernée les violations de données susceptibles de l'exposer à un risque élevé à ses droits et libertés.

- **Le droit de formuler des directives anticipées :** ce droit permet à la personne concernée de formuler des « directives anticipées » ou de définir ses souhaits sur la conservation,

l'effacement et la communication de leurs données personnelles après son décès. Il est posé par la Loi « Informatique et Libertés » mais n'est pas repris par le RGPD. Il a été intégré au projet de loi du 14 mai 2018 sur la refonte de la Loi Informatique et Libertés.

III. LES ACTEURS DU RPGD :

A. Le Responsable de traitement :

Le « Responsable de traitement » est l'un des acteurs principaux de la protection des données personnelles.

Il s'agit de la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui détermine les finalités et les moyens du traitement.

Il s'agit concrètement de l'entité collectant et traitant les données personnelles.
Plus précisément, il s'agira du représentant légal de cette entité.

Il peut exercer ses attributions « seul ou conjointement avec d'autres ».
Il peut ainsi exister un « Responsable conjoint de traitement » : il assume une responsabilité solidaire avec le Responsable de traitement à l'égard des personnes concernées.

Le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que le traitement est effectué conformément au Règlement.

Pour déterminer les mesures techniques et organisationnelles appropriées, il y a lieu de tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que de la probabilité et de la gravité des risques au regard des droits et libertés des personnes physiques.

Selon qu'il traite ou collecte des données pour le compte d'une entité, le Responsable de traitement a des obligations spécifiques pour garantir la protection des données qui lui sont confiées.

1. Le principe de responsabilité ou « Accountability » :

Le RGPD supprime l'obligation de déclaration de traitement auprès de la CNIL et permet de mettre en œuvre des traitements « librement » sauf si le traitement est réalisé dans le cadre d'une mission d'intérêt public (par exemple, protection sociale et santé publique) lequel devra toujours être soumis à l'autorisation de la CNIL.

L'une des innovations essentielles du RGPD est de privilégier « l'autocontrôle » de l'entreprise.

Selon le principe d' « accountability », l'entreprise doit être « responsable » du respect des principes généraux relatifs à la collecte et au traitement des données personnelles : **elle doit être en mesure de démontrer que ces principes ont été respectés.**

Selon ce principe, le responsable du traitement doit adopter les mesures techniques et organisationnelles appropriées pour s'assurer, et avoir la possibilité de démontrer, que le traitement est effectué conformément à la règlementation.
Ces mesures doivent, si nécessaire, être réexaminées et actualisées.

Les mêmes mesures doivent, à condition que cette exigence soit « proportionnée au regard des activité du traitement », comporter la mise en œuvre de « politiques appropriées en matière de protection des données ».

Il est possible qu'une entité soit dotée de « deux responsables de traitement » ou davantage.
Dans cette hypothèse, ils doivent établir un accord qui a pour objectifs :

- De déterminer de manière transparente leurs obligations respectives, notamment quant à l'exercice des droits des personnes concernées et la communication des informations qui doivent leur être fournies ;
- De refléter les rôles respectifs des responsables conjoints et leurs relations vis-à-vis des personnes concernées.

Mais la personne concernée a la possibilité d'exercer ses droits à l'égard de chaque responsable de traitement.

2. La protection des données « dès la conception » et la protection « par défaut » :

Le principe d' « Accountability » se trouve renforcé par deux nouvelles obligations :

- La protection des données dès la conception « **Privacy by design** » : les mesures techniques et organisationnelles doivent être mises en œuvre tant au moment de la détermination du traitement qu'au moment du traitement lui-même. Le traitement doit dès sa conception être conformes au RGPD et intégrer de façon effective les principes relatifs à la protection des données ;

- La protection des données « par défaut » « **Privacy by default** » : ces mesures doivent garantir que, « par défaut », seules les données personnelles nécessaires au regard de chaque finalité spécifique du traitement sont traitées.
  En particulier, les mesures en question doivent garantir que, « par défaut », les données personnelles ne soient pas rendues accessibles à un nombre indéterminé de personnes sans l'intervention de la personne concernée.
  Cette seconde obligation se rattache au principe de « minimisation des données ».

Parmi les techniques destinées à assurer le respect de ces dispositions figure la « **pseudonymisation**» des données.

Une « **donnée pseudonymisée** » est une donnée d'identification remplacée par un pseudonyme mais qui n'est pas une donnée anonyme.
Dans le cas-là, ces données « modifiées » de manière réversible sont soumises aux règles relatives à la protection des données.

Ce procédé se différencie de l'**anonymisation** en ce qu'il n'a pas pour résultat de supprimer toutes les informations identifiantes et de rendre pratiquement impossible la réidentification de la personne concernée.

Une « **donnée anonymisée** » est une donnée qui ne peut plus être reliée, de manière irréversible à un individu déterminé ou déterminable.
Dans ce cas-là, les règles relatives à la protection des données ne s'appliquent pas.

3. Analyse d'impact :

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

Mais le RGPD précise que **le traitement de données à caractère personnel de clients par un avocat ou un expert-comptable exerçant à titre individuel ne devrait pas être considéré comme constituant un traitement à grande échelle.**

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

C'est le cas lorsqu'en raison du type de traitement et, notamment, du recours à de nouvelles technologies, les droits et libertés des personnes sont exposées à un risque élevé, notamment :

- un traitement destiné au profilage des personnes ;
- un traitement à grande échelle de données sensibles, ou de données relatives aux condamnations pénales et aux infractions ;
- la surveillance systématique d'une zone accessible au public.

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

B. La sous-traitance :

Selon 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 les données à caractère personnel pour le compte du responsable de traitement*".

Il s'agit par exemple d'un comptable, un éditeur de logiciel, un hébergeur ou toute autre personne qui sera chargée de traiter les données personnelles pour le compte du Responsable de traitement.

Le sous-traitant doit présenter des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles permettant de répondre aux exigences du règlement et d'assurer la protection des droits de la personne concernée.

L'intervention d'un sous-traitant est généralement matérialisée par un contrat de sous-traitance qui définit :

- l'objet, la durée, la nature et la finalité du traitement sur lequel il porte ;
- le type de données personnelles et les catégories de personnes concernées ;
- les obligations et les droits du responsable du traitement.

A ces éléments principaux, doivent s'ajouter des clauses qui prévoient, notamment, que le sous-traitant :

- ne traite les données personnelles que sur « instruction documentée » du responsable du traitement ;
- veille à ce que les agents autorisés à traiter des données personnelles, s'engagent à respecter une obligation de confidentialité ou soient soumis à une telle obligation ;
- prend toutes les mesures destinées à assurer la sécurité des données personnelles ;
- aide le responsable du traitement à s'acquitter de ses obligations dans le cadre de l'exercice des droits ouverts à la personne concernée, ainsi que dans le domaine de la sécurité des données et de la réalisation de l'analyse d'impact ;
- met à la disposition du responsable du traitement toutes les informations propres à démontrer qu'il a respecté ses obligations et permettant d'effectuer des audits.

Le sous-traitant doit également faire connaître « immédiatement » au responsable du traitement si une instruction reçue de ce dernier constitue, selon lui, une violation de la réglementation.

D'une manière générale, le RGPD étend au sous-traitant l'application du nouveau principe d'Accountability à l'égard du responsable du traitement.

Le sous-traitant a aussi la possibilité de recruter un autre sous-traitant pour exercer des activités de traitement spécifiques mais doit, dans ce contexte, obtenir **préalablement** une autorisation spécifique ou générale du responsable de traitement.

Le sous-traitant de second rang se trouvera alors soumis aux mêmes obligations que le premier en matière de protection des données.

S'il ne respecte pas ses obligations, le sous-traitant principal demeure pleinement responsable de l'exécution des obligations incombant au sous-traitant de second rang.

Les cabinets d'avocats et d'experts-comptables sont pour la plupart déjà liés par des contrats avec des « sous-traitants ».
Ils doivent donc les interroger sur les garanties et mesures qu'ils ont mis en place afin d'assurer la conformité au RGPD.

Dans le cas où le cabinet identifie des lacunes dans les mesures mises en place par le sous-traitant, il devra conclure un avenant au contrat fin de combler lesdites lacunes.

C. Le Délégué à la Protection des données (« Data Protection Officer » ou DPO)

Aux termes de l'article 37 du RGPD, les responsables de traitement et les sous-traitants devront obligatoirement désigner un Délégué à la Protection des données :

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

En dehors de ces cas, la désignation d'un DPO sera bien sûr possible et même recommandée, notamment au sein des Cabinets d'avocats et d'experts-comptables.

Il n'existe pas de seuil en termes d'effectifs qui rend obligatoire la désignation du DPO, même si le RGPD exclue, pour l'heure, une désignation d'un DPO pour les avocats et experts-comptables exerçant à titre individuel.

Le DPO est désigné :

- sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données,
- ainsi que de sa capacité à exercer les missions qui lui sont confiées.

Un groupe d'entreprises peut désigner un seul délégué à condition qu'il soit « facilement joignable à partir de chaque lieu d'établissement ».

Ses coordonnées doivent être publiées et communiquées à l'autorité de contrôle.

Il peut appartenir au personnel de l'entreprise responsable du traitement ou de l'entreprise sous-traitante.
Il peut aussi être recruté à l'extérieur par la voie d'un contrat de service.

Il est soumis au **secret professionnel ou à une obligation de confidentialité**.

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le DPO est principalement chargé de :

- informer et conseiller le responsable de traitement ou le sous-traitant ainsi que leurs employés;
- s'assurer du respect du règlement et du droit nationale en matière de protection des données;
- conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et en vérifier l'exécution ;
- coopérer avec la CNIL et être le point de contact de celle-ci.

Le DPO doit notamment :

- s'informer sur le contenu des nouvelles obligations ;
- sensibiliser les décideurs sur l'impact de ces nouvelles règles ;
- réaliser l'inventaire des traitements de données de l'organisme
- concevoir des actions de sensibilisation
- piloter la conformité en continu.

En conséquence, la personne qui agit en tant que DPO endossera des responsabilités importantes.

Les personnes concernées peuvent saisir le DPO de toutes les questions relatives au traitement de leurs données personnelles et à l'exercice des droits que leur ouvre le règlement.

L'entreprise se voit imposer, quant à elle, diverses obligations destinées à faciliter l'activité du DPO et à garantir son indépendance, et doit notamment :

- associer le DPO, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données personnelles ;
- lui fournir les ressources nécessaires pour exercer ses missions ;
- lui ouvrir l'accès aux données personnelles et aux opérations de traitement ;
- lui permettre d'entretenir ses connaissances spécialisées ;
- veiller à ce que le DPO ne reçoive aucune instruction en ce qui concerne l'exercice de ses missions ;
- s'abstenir de relever le délégué de ses fonctions ou de le pénaliser pour des raisons liées à l'exercice de ses missions ;
- si le DPO exécute d'autres tâches, comme il en a la possibilité, veiller à ce qu'il n'en résulte aucun conflit d'intérêts.

Le DPO prendra la place du correspondant à la protection des données personnelles (dit «

correspondant informatique et libertés » ou CIL) dont les administrations et les entreprises avaient la faculté de se doter.

Sur ce point, il sera rappelé que l'Avocat peut être désigné comme CIL d'une entreprise.

L'article 6.3.3 du RIN précisait que l'Avocat – CIL **était déjà soumis à 2 devoirs qui ne s'imposent pas au CIL non avocat :**

- le devoir de non-dénonciation de son client
- le devoir de démission en cas de conflit d'intérêt.

Le RGPD a entraîné la modification de la rédaction de l'article 6.3.3 du RIN qui prévoit désormais que :

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

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

Désormais, l'avocat **doit refuser** de représenter les clients pour lesquels il exercé ou a exercé la mission de CIL dans les procédures mettant en cause le responsable des traitements afin d'éviter toute situation de conflit d'intérêt ou de violation du secret professionnel.

D. La CNIL : Autorité de contrôle et de sanction

Le RGPD impose à chaque Etat membre de l'Union d'instituer une ou plusieurs « autorités publiques indépendantes » (APD), également dénommées « autorités de contrôle », chargées de « surveiller » l'application de ses dispositions.

En France, la CNIL reste « l'autorité de contrôle ».

Elle pourra réaliser des enquêtes, accorder des autorisations et rendre des avis.

La CNIL peut réaliser

- Des contrôles sur place,
- Des contrôles sur pièces,
- Des auditions,
- Des contrôles en ligne.

Le Responsable du traitement doit être informé de :

- la mise en œuvre du contrôle et son objet,
- l'identité et la qualité des personnes contrôlées,
- le droit d'opposition existant le cas échéant : il est en effet possible de s'opposer au contrôle. La CNIL ne pourra maintenir son contrôle qu'après une autorisation du Juge des libertés et de la détention qui doit statuer dans les 48 heures.
  Le principal motif d'opposition à contrôle est le secret professionnel et il est nécessaire de rappeler son fondement légal ainsi que les données qui sont couvertes par ce secret.
  Il sera relevé que ce droit d'opposition à contrôle n'existe pas si le contrôle intervient sans information et sur autorisation préalable du Juge des Libertés et de la détention **en cas d'urgence, de risque de destruction ou de dissimulation de documents**.

Il doit être informé **8 jours au plus tard avant le contrôle sur place ou, en cas d'absence, 8 jours suivant le contrôle.**
Mais elle pourra également adopter diverses mesures correctrices à l'encontre des responsables de traitement et des sous-traitants.

Au titre des **sanctions administratives**, la CNIL peut notamment :

- Prononcer un avertissement si le traitement est susceptible de violer le RGPD ;
- Mettre en demeure l'entreprise de rendre les opérations de traitements conformes au RGPD ;
- Limiter temporairement ou définitivement un traitement ;
- Suspendre les flux de données ;
- Ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- Ordonner la rectification, la limitation ou l'effacement des données
- Prononcer des sanctions pécuniaires.

Les sanctions pécuniaires devront être effectives, proportionnées et dissuasives.
Elles peuvent être prononcées en complément des mesures correctrices que l'autorité de contrôle a le pouvoir d'adopter, ou encore à la place de ces mesures.

En revanche, les éventuelles sanctions pénales ne devraient pas pouvoir se cumuler avec les mesures correctrices et les amendes administratives.

Le RGPD innove en fixant le **plafond** des **sanctions pécuniaires**.

Deux plafonds sont prévus en fonction de la nature des manquements.

- **2% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise ou 10 millions d'euros** (le montant le plus élevé des deux doit être retenu) : pour les manquements au principe de Privacy by design, aux obligations en matière d'analyse d'impact, de tenue de registre, de sous-traitance, de sécurité, etc ;

- **4% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entreprise ou 20 millions d'euros** (le montant le plus élevé des deux doit être retenu) : pour les manquements aux droits des personnes, aux principes de loyauté, de licéité, aux obligations en matière de protection du consentement, etc.

Ces sanctions doivent être proportionnées en fonction de la gravité, la nature et la durée du manquement aux obligations du RGPD.

Outre les risques pécuniaires, les sanctions peuvent faire l'objet d'une **publicité**.

Cette publicité des décisions de la CNIL entraine un risque pour la réputation du cabinet.

La violation des données personnelles peut également faire l'objet de **sanctions pénales prononcées par le juge répressif sur le fondement du Code pénal**.

En effet, le Code pénal édicte **19 incriminations**, notamment :

- Le fait de « procéder ou faire procédure à un traitement (…) incluant parmi les données sur lesquelles il porte le numéro d'inscription au répertoire national d'identification des personnes physiques NIR (numéro de sécurité sociale) » (article 226-16-1 du Code pénal) ;
- « Le fait de collecter à caractère personnel par un moyen frauduleux, déloyal ou illicite » (article 226-18 du Code pénal),
- « le fait y compris par négligence, de procéder ou faire procéder à un traitement qui a fait l'objet d'une injonction de cesser le traitement ou d'un retrait d'autorisation » (article 226-16 alinéa 2 du Code pénal) ;
- Le défaut de sécurité,
- Le détournement de finalité.

Certaines de ces infractions constituent des délits ou des contraventions de 5ème classe.
Les délits sont réprimés par des peines pouvant aller jusqu'à 5 ans d'emprisonnement et 300.000 euros d'amende.

Enfin, la personne concernée dont les données personnelles ont été violées peut également agir en responsabilité civile contre le responsable de traitement ou le sous-traitant en réparation du préjudice subi.

Selon les cas, la personne concernée pourra agir **solidairement** contre le responsable du traitement et le sous-traitant.
D'où l'importance de bien déterminer dans le contrat de sous-traitance les rôles et obligations de chacun.

PARTIE 2 – SE METTRE EN CONFORMITE AVEC LE RGPD

Il a été indiqué que le RGPD s'applique « *au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier* »

Or, tous les cabinets d'avocats et d'expertise comptable, dans le cadre de leur organisation interne, collectent, utilisent ou procèdent à des opérations sur des informations se rapportant à des personnes physiques identifiées ou identifiables.

Les données qui peuvent être collectées par les cabinets d'avocats et d'expertise-comptable sont principalement relatives ou nécessaires à

- La gestion du personnel,
- La gestion des clients,
- La gestion des fournisseurs,
- La gestion de la comptabilité,
- La gestion de la paie.

Ils doivent donc se conformer à l'ensemble des règles réaffirmées ou nouvelles relatives à la protection des données personnelles.

Ils seront ainsi « responsables de traitement » et ont l'obligation de s'assurer que les prestataires informatiques, agissant en qualité de sous-traitants, ont mis en place les mesures techniques et organisationnelles adaptées permettant de respecter la sécurité et la confidentialité des données.

En ce qui concerne les experts-comptables, la nature des leurs missions et interventions aura une incidence sur leur statut.

Si le cabinet d'expertise-comptable collecte et traite des données personnelles dans le cadre de la finalité qu'il a déterminée et selon les moyens qu'il a choisis de mettre en œuvre (par exemple la gestion de son personnel), il sera alors Responsable de traitement.

S'il collecte des données personnelles dans le cadre d'une mission qui lui est confiée par un client (par exemple l'établissement des bulletins de paie ou la comptabilité), il sera alors « sous-traitant » et le client – entité sera le Responsable de traitement.

Enfin, le cabinet d'expertise-comptable (et parfois les cabinets d'avocats) peut être chargé par son client d'une mission d'audit.
Dans ce cadre, c'est le cabinet qui va déterminer les finalités des traitements à réaliser et les moyens à mettre en œuvre.

Il sera alors considéré comme Responsable conjoint du traitement et soumis à l'ensemble des obligations et des responsabilités pesant sur le Responsable de traitement.

Il convient donc de bien préciser par des lettres de missions les rôles des cabinets d'expertise-comptable pour éviter au maximum cette responsabilité solidaire de Responsable de traitement.

Il convient donc d'exposer les règles relatives aux principaux traitements de données personnelles qui peuvent être réalisées par les cabinets d'avocats et d'expertise-comptable.

A. La tenue du Registre des activités de traitement :

En contrepartie de la suppression de la formalité préalable de déclaration d'un traitement de données personnelles, le RGPD impose désormais à chaque responsable de traitement a, en principe, **de tenir un registre des activités exercées sous sa responsabilité**.

Il a pour principal objectif de permettre au Responsable de traitement d'être en mesure de justifier qu'il s'est conformé aux règles applicables à la protection des données personnelles et donc au principe d' « Accountability ».

La même obligation de tenue d'u Registre des activités de traitement s'impose au sous-traitant.

Cette obligation de tenir un Registre des activités de traitements ne s'impose qu'aux entreprises comptant **plus de 250 salariés**.

Mais l'obligation de tenue de ce Registre subsiste si :

- le traitement comporte un risque pour les droits de la personne concernée ;
- il ne présente pas un caractère « occasionnel » :
- il porte sur des données sensibles ou des données relatives aux condamnations pénales et aux infractions.

Ainsi, même si les cabinets d'avocats et d'experts-comptables ne sont pas directement concernés par cette obligation de tenir un Registre des activités de traitements, il est fortement recommandé qu'ils s'y conforment.

Qu'elle incombe au responsable du traitement ou à un sous-traitant, la tenue du registre des activités de traitement est soumise à certaines **règles communes** :

- le registre doit se présenter sous une forme écrite, y compris électronique ;
- l'entreprise principale ou sous-traitante a l'obligation de mettre le registre à la disposition de l'autorité de contrôle si cette dernière le demande.

La CNIL préconise de « cartographier » les traitements de données personnelles en se posant au préalable les questions suivantes :

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

Le registre des activités de traitement doit comporter les informations suivantes :

- le nom et les coordonnées du responsable du traitement, ainsi que, le cas échéant du responsable conjoint et du DPO ;
- les finalités du traitement ;
- une description des catégories de personnes concernées et des catégories de données personnelles ;
- les catégories de destinataires auxquels les données personnelles ont été, ou seront, communiquées ;
- le cas échéant, les transferts de données vers les pays tiers.
- les délais prévus pour l'effacement des données ;
- une description générale des mesures de sécurité techniques et organisationnelles.

B. Les principaux types de traitements de données personnelles :

1. Le traitement « RH » (Ressources humaines)

Le traitement « Ressources Humaines » ou RH est celui réalisé par les cabinets d'avocats et d'experts-comptables dans le cadre du recrutement d'un collaborateur ou du personnel support (informaticien secrétaire…) la gestion de la paye, et la gestion administrative du personnel.

Comme tout traitement de données personnelles, le Traitement RH doit respecter le principe de minimisation des données : le responsable de traitement ne doit collecter que les données adéquates pertinents et strictement nécessaires à la finalité du traitement.

Seules les données relatives à la qualification et l'expérience du candidat peuvent être collectées, soit des données permettant d'évaluer la capacité du candidat à occuper le poste proposé **:** diplômes, emplois précédents…

Il est donc interdit de :

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

Pour se conformer au RGPD, le Responsable de traitement doit insérer dans le Registre des Traitements une fiche dédiée à la gestion des ressources humaines qui doit comporter les éléments suivants :

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

Le Responsable de traitement doit également une politique de durée de conservation des données puisqu'elles ne peuvent être conservées que le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte.

Ainsi dans le cadre d'un « Traitement RH », les données personnelles relatives aux collaborateurs et salariés seront conservées le temps de présence dans le cabinet, augmenté des durées de prescription légale.

Comme tout traitement de données personnelles, les personnes concernées devront recevoir une information sur l'existence de ce traitement, sa finalité, la durée de conservation des données et les conditions d'exercice de ses droits, le droit de retirer son consentement à tout moment…
Cette information peut figurer sur les contrats de travail ou les contrats de collaboration.

Elles peuvent également faire l'objet d'un affichage ou d'une communication par courriel, notamment pour régulariser la situation auprès des collaborateurs ou salariés qui n'ont pas été correctement informés.

2. La gestion des clients :

Les données à caractère personnel qui peuvent être collectées auprès des clients sont celles qui correspondent à toutes les données nécessaires à la constitution du dossier du client, la défense de ses intérêts ou l'exécution des missions réalisées pour les clients.

Au regard de la diversité des domaines d'intervention de l'Avocat et des missions qui peuvent être confiées aux experts-comptables, ces données peuvent être très diverses et peuvent concerner des données relatives tant à la vie personnelle qu'à la vie professionnelle mais peuvent également concerner des données d'une particulière sensibilité.

Par exemple, un **avocat** peut être amené à collecter :

- des **données relatives aux condamnations pénales et aux infractions.** Le RGPD limite au maximum le traitement de ces données en exigeant qu'il soit, lorsqu'il est réalisé, entouré de garanties spécifiques et adaptés. Le Projet de refonte de la Loi « Informatique et Libertés » maintiendra l'exception de traitement de ces données fixée par le RGPD au profit des avocats en raison de la finalité de ce traitement : la mission de défense du client ;
- des **données sensibles** (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques ou appartenance syndicale, données génétiques, données biométriques, vie sexuelle ou orientation sexuelle) pour lesquelles le RGPD pose un principe d'interdiction de collecte et de traitement. Mais le RGPD prévoit une exception pour la collecte et le traitement de ces « données sensibles » au profit des avocats (notamment ceux spécialisés en droit de la santé ou en dommage corporel) dès lors que la donnée concernée soit strictement nécessaire à la constatation, l'exercice ou la défense d'un droit en justice pour son client.

L'**expert-comptable** va également collecter et traiter un nombre important d'informations dans le cadre des missions qui lui sont confiées par ses clients.

Il peut s'agir de **la mission d'établissement des bulletins de paie**.
Dans ce cadre, l'expert-comptable va utiliser les données personnelles des salariés des clients.
Pour établir les déclarations sociales (DADS-U ou DNS) l'expert-comptable vont ainsi devoir utiliser le NIR (numéro d'inscription au registre – déclaration de sécurité sociale).

Il pourra aussi avoir accès aux « données sensibles »

- pour la gestion des arrêts maladie, les fiches d'inscription aux mutuelles avec la mention des conjoints et des enfants couverts,
- le taux d'incapacité pour les déclaration AGEFIPH (déclaration annuelle obligatoire d'emploi des travailleurs handicapés, des mutilés de guerre et assimilés) ;
- s'il propose à ses clients une mission d'assistance à l'organisation des élections syndicales puisqu'il aura ainsi accès à l'appartenance syndicale des salariés du client ;

Si l'expert-comptable propose une **mission d'assistance au recrutement pour ses clients**, il devra être très attentif aux traitements des données contenues dans les CV et aux comptes-rendus d'entretien qui peuvent comporter des appréciations sur les candidats.

Lorsqu'il intervient dans le cadre de la **mission de tenue de la comptabilité et d'établissement des comptes annuels**, l'expert-comptable va ainsi collecter puis traiter des données concernant notamment les associés et les dirigeants de la structure avec la mention de leur rémunération (le cas échéant pour les sociétés cotées).

Dans le cadre de la **mission d'établissement des déclarations fiscales**, l'expert-comptable sera amené à traiter des données personnelles relatives aux personnes les mieux rémunérées de l'entité cliente (déclaration n°2067) ou bien encore les données des associés avec leurs adresses et numéro de sécurité sociale, la mention de dividendes versés et les intérêts qui leur ont été versés.

La DAS2 mentionne également le montant des honoraires, commissions, remises commerciales, droits d'auteurs ou d'inventeurs versés à des tiers qui peuvent être des personnes physiques (professions libérales ou BNC).

Enfin, les déclarations d'impôts sur les revenus des particuliers et les annexes (déclarations 2042, 2044 pour les revenus fonciers 2074 pour les plus-values mobilières et 2047 pour les revenus encaissés à l'étranger) l'impôt sur la fortune immobilière (IFI) impliquent également le traitement de données personnelles.

Les avocats et les experts-comptables sont régulièrement amenés à réaliser des **audits de clients ou pour le compte de clients** ou des **prestations de secrétariat juridique**.
Ces missions impliquent le traitement de données personnelles que ce soit au travers des informations relatives aux personnes physiques de la société auditée ou aux associés des entités dont le secrétariat juridique est réalisé.

Comme tout traitement de données personnelles, les données collectées dans le cadre de la gestion – clients doivent respecter le principe de minimisation qui impose de ne collecter auprès des clients que des données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

Le client a souvent tendance à communiquer un nombre important d'information.
Pour se conformer au mieux au principe de minimisation, il est recommandé de tenter d'orienter son client lorsqu'il fournit des données personnelles vers celles qui sont nécessaires à la mission qu'il confie à l'avocat ou l'expert-comptable.

Comme pour le traitement RH, le responsable de traitement devra donc insérer dans le Registre des activités de traitement, une fiche dédiée à la gestion des clients qui doit comporter les éléments suivants :

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

Comme pour tout traitement, le responsable de traitement doit également définir une durée de conservation des données collectées et traitées dans le cadre de la gestion des clients puisqu'elles ne peuvent être conservées que **le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte**.

Généralement les données relatives aux clients peuvent être conservées le temps de la relation contractuelle.

Au-delà, les données devraient être archivées pendant le délai sous lequel une action en responsabilité civile professionnelle pourrait être introduite par le client, avant une suppression définitive des données.

Les personnes concernées par ce traitement des données personnelles collectées et traitées dans le cadre de la gestion de clients et de prospects doivent naturellement recevoir une information sur l'existence de ce traitement, sa finalité, la durée de conservation des données et les conditions d'exercice de ses droits, le droit de retirer son consentement à tout moment…

Ces informations peuvent figurer au **sein de la convention d'honoraires ou de la lettre de mission.**

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

3. Les sites Internet :

Les avocats et les experts-comptables peuvent créer des sites Internet dans le cadre de leurs activités professionnelles afin de promouvoir leurs cabinets, présenter les membres des cabinets, exposer leurs compétences ou publier des articles.

Mais le site Internet peut aussi permettre de collecter des données à caractère personnel par divers moyens :

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

Dans la mesure où il s'agit d'un traitement, le Responsable de traitement devra insérer dans le Registre des activités de traitement, une fiche dédiée au traitement des données sur le site Internet.

De manière plus générale, les sites Internet doivent également être mis en conformité avec les nouvelles règles fixées par le RGPD.

C’est notamment la raison pour laquelle nous recevons depuis le 25 mai 2018 des e-mails des sites Internet sur lesquels nous avons créé des comptes nous informant de la mise à jour de leur « Politique de confidentialité ».

Ils doivent désormais comporter les mentions suivantes :

- les mentions légales en vertu 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 l'inscription est requise)
    - Coordonnées postales, téléphoniques et électroniques du cabinet
    - Nom et coordonnées du directeur de la publication du site
    - Nom, raison sociale, adresse et numéro de téléphone de l'hébergeur du site

- les mentions obligatoires en vertu des règles déontologiques applicables :
    - Précision de la qualité (avocat, expert-comptable)
    - Identification de la personne (associés) et du cabinet
    - Fourniture des informations sur sa localisation
    - Eléments permettant de le joindre (téléphone, fax, courriel)
    - Précision sur la structure d'exercice à laquelle il appartient
    - le cas échéant, précision du réseau dont l'avocat ou l’expert-comptable est membre

- les mentions d'informations issues des articles 13 et 14 du RGPD
    - l'identité et les coordonnées du responsable du fichier
    - les coordonnées du Délégué à la Protection des données
    - la finalité et la base juridique du traitement
    - les intérêts légitimes poursuivis s'il s'agit de la base légale du traitement
    - les destinataires ou les catégories de destinataires
    - la durée de conservation des données
    - les éventuels transfert de données vers des pays hors UE
    - le droit de retirer son consentement à tout moment s'il s'agit de la base légale du traitement
    - le droit d'introduire une réclamation auprès d'une autorité de contrôle
    - les informations sur le caractère réglementaire ou contractuel du traitement s'il s'agit de la base du traitement

- les mentions d'informations relatives aux cookies
    - les finalités des cookies,
    - le recueil du consentement des utilisateurs via les « bandeaux de consentement »
    - les possibilités de refuser les cookies.

Sur ce dernier point, il est rappelé qu'un cookie est un traceur déposé et lu lors de la consultation du site Internet du cabinet, de la lecture d'un courriel ou de l'installation ou l'utilisation d'un logiciel.

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

L'utilisation des cookies sur le site Internet du cabinet doit aussi être rendue conforme au RGPD.
Il convient dans un premier temps de vérifier la présence effective de cookies sur les sites Internet par le biais du service informatique, des prestataires ou en vérifiant les outils utilisés.

Dans un second temps, il est nécessaire de déterminer les types de cookies utilisés sur le site Internet. Beaucoup de cookies requièrent le consentement de l'utilisateur.

Ensuite, il convient de déterminer les types de cookies utilisés sur le site Internet.

- les cookies publicitaires,
- les cookies "réseaux sociaux" générés par le bouton de partage lorsqu'ils collectent des données personnelles sans consentement des personnes concernées
- certains cookies de mesure d'audience.

Dans ce cas, le consentement doit être préalable à l'insertion ou à la lecture de cookies.

Tant que le client n'a pas donné son consentement, ces cookies ne peuvent pas être déposés ou lus sur son terminal.

4. La lutte contre le blanchiment et le financement du terrorisme :

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

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

L'avocat ou l'expert-comptable qui « noue une relation d'affaires » avec un client doit exercer une vigilance constante pendante 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.

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 » et actualiser ces informations pendant toute la durée de la relation.

Ainsi, concernant une personne physique, l'avocat ou l'expert-comptable doit se voir présenter l'original d'un document officiel en cours de validité comportant la photographie du client (articles L 561-5 et suivants et articles R 561-6 et suivants du Code monétaire et financier).

Les mesures de vigilance et d'identification doivent être renforcées lorsque l'opération paraît :

- particulièrement complexe
- d'un montant inhabituellement élevé
- ou ne paraît pas avoir de justification économique
- ou d'objet licite.

Dans un tel cas, il faut alors se renseigner et obtenir des éléments complémentaires en posant des questions complémentaires.
Si ces informations complémentaires ne sont pas jugées suffisantes, il faut alors consigner par écrit et conserver les caractéristiques de l'opération, soit les informations recueillies et documentées 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 ci-dessus (complexité, montant important, justification économique ou objet licite)
- l'identité du client donneur d'ordre et du ou des ayants-droits économiques en précisant pour chacun, le nom, l'adresse, la nationalité et la profession.

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, s'exprime ici pleinement.

Les données relatives à l'identité des clients habituels ou occasionnels (ainsi que les documents et supports) doivent être conservées pendant 5 ans à compter de la cessation de la relation avec le client.

Il en va de même pour les documents relatifs aux opérations réalisées.

5. Les systèmes de vidéosurveillance et de vidéoprotection :

Il convient de distinguer la vidéoprotection de la vidéosurveillance puisque chacune a son propre régime :

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

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

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

Selon le lieu où les caméras sont installées, le régime applicable diffère, étant précisé que la CNIL reste compétente.
Les dispositifs soumis aux dispositions du Code de la sécurité intérieure, malgré le RGPD, restent soumis à l'obligation d'autorisation de la Préfecture du département (Préfet de Police à Paris), par exemple :

- une caméra située dans un lieu public ou ouvert au public avec un enregistrement ou une conservation d'images dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques (Salle d'attente, immeuble du cabinet, hall d'entrée), doit faire l'objet d'une autorisation préfectorale;
- une caméra située dans un lieu public ou ouvert au public sans enregistrement ni conservation d'images dans des traitements informatisés ou des fichiers structurés qui permettent d'identifier des personnes physiques (Salle d'attente, immeuble du cabinet, hall d'entrée), doit faire l'objet d'une autorisation préfectorale.

Pour les autres dispositifs (par exemple une caméra située dans le cabinet fermé au public (bureaux, réserves, couloirs...), la déclaration préalable auprès de la CNIL a été supprimée par le RGPD.

Mais le responsable de traitement devra insérer dans le Registre des activités de traitement, une fiche dédiée à la vidéosurveillance et à la vidéoprotection.

Comme pour chaque traitement, les personnes concernées, à savoir les clients, les membres du cabinet, les confrères ou encore les prestataires, doivent être informés de l'existence du dispositif mis en place.

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

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

Lorsqu'il en existe au sein des cabinets, les instances représentatives du personnel 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.

Les images enregistrées par les caméras de vidéoprotection ou de vidéosurveillance ne peuvent être visionnées que par les seules personnes habilitées dans le cadre de leurs fonctions (associé ou personne responsable de la sécurité).

Ces personnes doivent être particulièrement formées et sensibilisées aux règles encadrant la mise en place d'un tel système.

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

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

C. Les bonnes pratiques de sécurité des données :

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

En effet, les avocats et les experts-comptables sont soumis au secret professionnel.
Cette obligation renforce la nécessité de mettre en place des mesures de sécurité dans les cabinets d'avocats et d'experts-comptables puisqu'en cas de violation des données personnelles, c'est le secret professionnel qui est violé.
L'enjeu de la sécurité n'est donc pas anodin.

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

- limiter l'accès au cabinet,
- ne pas stocker ou archiver des dossiers ou des documents contenant des données personnelles dans des bureaux accessibles à tous (privilégier les bureaux fermés à clés);
- installer des alarmes dans les locaux du cabinet ;
- vérifier la sécurité du système d'information sur lequel sont stockés les dossiers sous format numérique (parefeu, mots de passe robustes pour y accéder, habilitations...)…
- ...

Il est également possible de prévoir, à titre de sécurité, un encadrement des conditions d'accès à Internet dans les cabinets et de mettre en place des filtres pour bloquer l'accès à certains contenus (pédophiles ou pornographiques) ou limiter le téléchargement de logiciels…

Mais, il convient également de s'assurer que les mesures de sécurité mises en place dans les cabinets ne soient pas détournées de leur finalité principale.

Ainsi, si les cabinets mettent en place un logiciel permettant de calculer le temps passé par un collaborateur sur un dossier, il ne pourra en aucun cas être utilisé par l'employeur pour contrôler son activité réelle…

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

Il est notamment conseillé de :

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

- **gérer les habilitations et sensibiliser les utilisateurs :**
    - déterminer les personnes qui sont habilitées à accéder aux données personnelles,
    - supprimer les permissions d'accès obsolètes
    - rédiger une charte informatique et l'annexer au règlement intérieur s'il en existe un.

- **sécuriser l'informatique mobile :**
    - prévoir des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clés USB, CD, DVD...)
    - éviter d'y stocker des données personnelles sensibles des clients.

- **sauvegarder et prévoir la continuité de l'activité** : mettre en place des sauvegardes régulières, **stocker** les supports de sauvegarde dans un endroit sûr...

D. La procédure en cas de violation des données personnelles :

Une violation de données personnelles est une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Comme indiqué, il s'agit également pour les avocats et les experts-comptables d'une violation du secret professionnel.

Cette violation des données personnelles doit être **notifiée à la CNIL dans les meilleurs délais et si possible au plus tard dans les 72 heures après que le Responsable de traitement en a pris connaissance.**

Cette notification doit, entre autres choses, préciser :

- la nature de la violation des données personnelles (catégories et nombre approximatif de personnes et d'enregistrements de données concernés)
- le nom et les coordonnées du Délégué à la Protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues;
- les conséquences probables de la violation ;
- les mesures prises ou à prendre en vue d'atténuer les éventuelles conséquences négatives ou de remédier à la violation.

En outre et si elle est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, cette violation des données personnelles doit également être communiquée par le Responsable de traitement à la personne concernée **dans les meilleurs délais.**

Cette information à la personne concernée

- décrit, en des termes clairs et simples, la nature de la violation ;
- contient les autres informations dont la notification à l'autorité de contrôle est obligatoire : nom et coordonnées du DPO ou d'un autre « point de contact », conséquences probables de la violation, remèdes à celle-ci.

Si cette communication à la personne concernée d'une violation de ses données personnelles n'est pas réalisée, la CNIL peut imposer aux cabinets d'avocats ou d'experts-comptables, après avoir examiné le risque résultant de cette violation, enjoindre le responsable de traitement de procéder à cette communication.

Si les avocats et les experts-comptables recourent à des sous-traitants, ceux-ci sont également soumis à l'obligation de notifier au Responsable de traitement toute violation de données personnelles dans les meilleurs délais après en avoir pris connaissance.

Ce point doit donc être expressément prévu dans les contrats avec les sous-traitants.

La violation des données personnelles est susceptible, si elle permet à la CNIL de constater la non-conformité du cabinet au RGPD, d'entraîner le prononcé d'une sanction administrative (10 millions d'euros, ou, dans le cas d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent).

COMMENT SE METTRE EN CONFORMITE AVEC LE RGPD

INTRODUCTION

- Un traitement de données

  Essentiellement à travers un traitement informatique ou via internet, mais pas exclusivement (fichier manuel)

- Des données personnelles.

  C'est-à-dire concernant uniquement des personnes physiques et non des entreprises ou des entités juridiques.

- La question du consentement.

  Toutes les entités qui s'adressent directement à des personnes physiques ont du ou doivent demander leur consentement explicite pour traiter de leurs données personnelles (fournisseurs d'accès internet, toute entité réalisant un suivi régulier et systématique des personnes à grande échelle …)

- Le consentement n'est pas demandé lorsque celui qui traite les données personnelles le fait en vertu d'un contrat.

- Que les données personnelles soit traitées sur la base du consentement ou en vertu d'un contrat, celui qui collecte ces données est soumis à une obligation de protection de ces données.

- Exemples de traitement de données personnelles dans un cabinet d'expertise comptable :

  . La paie

  . La production de liasses fiscales (information sur les 5 ou 10 rémunérations les plus élevées)

  . Le fichier clients (nom, téléphone, mail, numéro d'identification des Responsables de l'entreprise)

LES ETAPES DE LA MISE EN CONFORMITE

1) METTRE EN PLACE OU DESIGNER UN RESPONSABLE DES DONNEES PERSONNELLES AU SEIN DU CABINET OU DE L'ENTREPRISE

   C'est obligatoire uniquement pour certaines structures qui traitent de fichiers à grande échelle : ministères, banques, compagnies d'assurances, opérateurs téléphoniques, fournisseurs d'accès à internet …), mais préconisé dans chaque entreprise.

Ce Responsable doit pouvoir s'appuyer sur les ressources internes de l'entreprise (juridiques et informatiques essentiellement et sur les organes de gouvernance)

A noter que ce Responsable peut être extérieur à l'entreprise et exercer cette fonction pour plusieurs entreprises.

2) AUDITER LES TRAITEMENTS DE DONNEES PERSONNELLES EXISTANTS

Il s'agit de procéder à l'inventaire des traitements de données personnelles, examiner leurs bases juridiques ou la nécessité d'un consentement.

Le Conseil Supérieur de l'Ordre des Experts-comptables a établi un référentiel en 12 points, essentiellement descriptif, pour s'assurer du respect de la règlementation :

- Recensement des traitements par finalités : quel est l'objet des traitements, toutes les données sont-elles nécessaires ?
- Catégories des données collectées
- Qui sont les destinataires des données
- Quels sont les outils de mise en œuvre des traitements
- Quelle est l'origine des données
- Comment se fait la mise à jour et quelle est la durée de conservation des données

- Comment sont informées les personnes concernées
- Comment s'exerce leurs droits pour les personnes concernées (droit à rectification, droit à l'oubli, droit à la portabilité…)
- Examiner la sécurité des données
- Y-a-t-il des transferts de données vers des pays tiers ?
- La vérification éventuelle des déclarations antérieures faites auprès du CNIL
- La Responsabilité (accountability)

L'audit permet de faire une évaluation des risques, qui s'ils sont considérés comme élevés, pourront nécessiter une étude d'impact des données (PIA : Privacy Impact Assessment)

3) L'AUDIT TECHNIQUE ET L'AUDIT DES PRESTATAIRES

- L'audit technique

Evaluer le niveau de sécurité en conformité avec les exigences du RGPD : Collecte, transmission, conservation, traitement des données personnelles.

Risque de destruction, de perte, d'altération, de divulgation non autorisée de données personnelles.

D’une manière générale cet audit recoupe l’évaluation du système de sécurité informatique de façon à détecter des failles et préconiser des améliorations.

Le Conseil Supérieur des Experts-comptables propose un questionnaire pour réaliser cet audit technique (annexe point12), sous différents critères :

. Gouvernance, politiques internes , procédures

. Transferts de données

. Gestion des risques et politique de sécurité

. Gestion des utilisateurs

. Protection des accès

. Contrôle des accès au réseau .

. Chiffrement des données

. Site Web

- L’audit des sous-traitants

  Mesures mises en place par les sous-traitants en matière de gestion des données : utiliser le même questionnaire d’audit technique et se faire remettre une attestation de conformité au RGPD.

  Le Conseil Supérieur préconise d’insérer des clauses dans les contrats de sous-traitance (annexe 6,7 et 8)

4) ARRETER UN PLAN D'ACTION

Les audits effectués permettent de déterminer les actions à mettre en œuvre pour respecter les nouvelles règles, notamment :

- Concernant le personnel :

  . Une Charte informatique (annexe 4)

  . Des mentions d'information (annexe 1)

  . Des clauses relatives au contrat de travail (annexe 5)

- Concernant les tiers et sous-traitants

  (Annexe 1 et sous-traitants annexe 6,7 et 8)

- Concernant le Cabinet :

  . Tableau d'évaluation des risques d'atteinte à la sécurité des données personnelles (annexe 3)

  . Clauses à insérer dans les lettres de mission (annexe 9)

  . Procédure de demande d'exercice des droits (annexe 13)

  . Procédure de gestion des failles de sécurité (annexe 1)

-

5) CREATION DU REGISTRE DES TRAITEMENTS, SI NECESSAIRE

Le registre de traitement est obligatoire pour toutes les entreprises de plus de250 salariés.

Pour les autres il est nécessaire si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées.

Le registre (modèle annexe 15) contient un certain nombre d'informations sur les traitements de données personnelles, qui sont :

- Qui ? : noms des responsables de traitement ou délégué à la protection des données
- Quoi ? : catégories de données traitées et identification des risques (données sensibles)
- Pourquoi ? : finalités pour lesquelles les données sont collectées ou traitées
- Où ? : pays dans lesquels les données sont hébergées ou transférées
- Jusqu'à quand ? durée de conservation des données par catégories (annexe 2)
- Comment ? : Mesures de sécurité pour minimiser les risques

6) ORGANISER LES PROCEDURES INTERNES ET DOCUMENTER LES ACTIONS MENEES

Il s’agit de répondre à l’obligation prévue par le RGPD de responsabilité (accountability).

Il s’agit de démontrer que des mécanismes et procédures internes ont été mis en œuvre pour le respect des règles relatives à la protection des données et de regrouper la documention nécessaire à cet effet.