Préambule

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

L'article 2 alinéa 2 de la loi informatique et libertés dispose que :

« Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ». ex. : nom, n° d'immatriculation, n° de téléphone, photographie, éléments biométriques tels que l'empreinte digitale, ADN, informations permettant de discriminer une personne au sein d'une population telles que, par exemple, le lieu de résidence, la profession, le sexe, l'âge, etc.).

Il peut en effet s'agir d'informations qui ne sont pas associées au nom d'une personne mais qui peuvent permettre de l'identifier et de connaître ses habitudes ou ses goûts. Exemples : « Le propriétaire du véhicule 3636AB75 est abonné à telle revue » ou encore « l'assuré social 1600530189196 va chez le médecin plus d'une fois par mois ».

Qu'est-ce qu'une donnée sensible ?

Parmi les données à caractère personnel, il existe une sous-distinction liée aux données sensibles. Les données sensibles sont celles qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou sont relatives à la santé ou à la vie sexuelle de celles-ci. Par principe, la collecte et le traitement de ces données sont interdits. Cependant, dans la mesure où la finalité du traitement l'exige, les traitements pour lesquels la personne concernée a donné son consentement exprès et les traitements justifiés par un intérêt public après autorisation de la CNIL ou décret en Conseil d'Etat ne seront pas soumis à cette interdiction.

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

L'article 2 alinéa 3 de la loi informatique et libertés dispose que : « Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou

la destruction ».

Gros plan sur les 5 grands principes à respecter en matière de données à caractère personnel

Avant de parler du RGPD en général, il est utile de revenir sur ce qui constitue, depuis la loi dite informatique et libertés de 1978, le socle des principes en matière de données à caractère personnel repris dans le texte européen qu'est le RGPD.

L'article 6 du RGPD dispose, en effet, que : «

« 1. Les données à caractère personnel doivent être :

a) **traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);**

b) **collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités;** le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) **adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);**

d) **exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);**

e) **conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées;** les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée **(limitation de la conservation);**

f) **traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);** »

La loi *« Informatique et Libertés »* et le RGPD ont donc défini les principes à respecter lors de la collecte, du traitement et de la conservation de ces données. La loi prévoit également un certain nombre de droits pour les personnes dont les données personnelles ont été recueillies.

1. **Le principe de finalité : une utilisation encadrée des fichiers**

Ce principe implique que les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions de l'entreprise ou de la personne physique responsable du traitement.

Le fichier ainsi constitué ne peut donc être utilisé à des fins commerciales ou politiques, sauf accord exprès du client ou de la personne.

Ce principe implique que les informations exploitées dans un fichier soient cohérentes par rapport à son objectif.

Ces données ne peuvent pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées.

Tout détournement de finalité est passible de 5 ans d'emprisonnement et de 300 000 euros d'amende.

> L'article 226-21 du Code pénal dispose, en effet, que : « Le *fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende* ».

Le principe de finalités déterminées est donc au cœur de la confiance que les personnes peuvent avoir dans les services de la société numérique. C'est grâce à ce principe que les données personnelles ne sont pas des marchandises comme les autres.

2. **Le principe de minimisation**

Ce principe découle directement du principe de finalité.

Il impose que seules doivent être enregistrées les informations et données personnelles adéquates, pertinentes et nécessaires pour assurer la mission poursuivie par l'entreprise.

Toutes celles qui ne sont pas en rapport avec cette mission seront considérées comme contraire aux principes de pertinence et de proportionnalité.

Il faut que la donnée collectée fasse corps avec le domaine d'activité de l'entreprise ou à défaut avec quelque chose dont cette entreprise pourrait légitimement indiquer à la CNIL qu'elle en avait besoin pour améliorer son service.

3. **Le principe de durée limitée de conservation des données**

Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation raisonnable doit être, le plus souvent, établie en fonction de la finalité de chaque fichier.

La CNIL préconise notamment une durée n'excédant pas 3 ans pour les données à caractère marketing et commercial relative à des prospects ou anciens clients. **Elles ne peuvent être conservées que pendant un délai de trois ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect.**

Au terme de ce délai de trois ans, le responsable de traitement peut reprendre contact avec la personne concernée afin de savoir si elle souhaite continuer à recevoir des sollicitations commerciales. En l'absence de réponse positive et explicite de la personne, les données devront être supprimées ou archivées conformément aux dispositions en vigueur et notamment celles prévues par le code de commerce, le code civil et le code de la consommation.

Le code pénal sanctionne la conservation des données pour une durée supérieure à celle qui a été déclarée de 5 ans d'emprisonnement et de 300 000 euros d'amende (article 226-20 du Code pénal).

Cela implique donc, dans l'hypothèse, d'une utilisation de donnée personnelle d'être en mesure de supprimer celles qui par l'effet du temps doivent l'être et de ne conserver que celles qui peuvent continuer à être traitées.

4. Le principe de sécurité et de confidentialité

1.1 Sécurité

L'article 32 du RGPD intitulé « sécurité du traitement » dispose que : *« Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques,* ***le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins*** *».*

En somme, il s'agit de comprendre que plus la sensibilité de la donnée sera avérée (ex : données médicales) et plus les mesures de sécurité attendues seront accrues. A l'inverse, des données personnelles classiques gérées par des sociétés tout aussi anodines pourront n'appeler que les mesures de sécurité élémentaires.

De façon générale, le responsable du traitement, est astreint à une obligation de sécurité : il doit prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation.

Les données contenues dans les fichiers ne peuvent être consultées que par les services habilités à y accéder en raison de leurs fonctions.

Il faut NOTAMMENT que l'entreprise veille à ce que chaque utilisateur ait un mot de passe individuel régulièrement changé et que les modalités d'accès soient précisément définies en fonction des besoins réels.

Le responsable du traitement doit prendre toutes les mesures pour empêcher que les données

soient déformées, endommagées ou que des tiers non autorisés y aient accès.

Exemple : S'il est fait appel à un prestataire externe, des garanties contractuelles doivent être envisagées.

Tout responsable de traitement informatique de données personnelles **doit adopter des mesures de sécurité physiques** (sécurité des locaux), **logiques** (sécurité des systèmes d'information) et **adaptées** à la nature des données et aux risques présentés par le traitement. Exemple : Protection anti-incendie, copies de sauvegarde, installation de logiciel antivirus, changement fréquent des mots de passe alphanumériques d'un minimum de 8 caractères.

Les mesures de sécurité doivent être adaptées à la nature des données et aux risques présentés par le traitement (Les banques et les opérateurs de télécommunications sont tenus à des mesures de sécurité plus importantes et plus lourdes qu'une PME.

Exemple : Authentification forte pour l'accès aux résultats d'examen, chiffrement des coordonnées bancaires transitant sur internet.

Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 euros d'amende (Article 226-17 du Code pénal).

4.2 Confidentialité

Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier.

Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des «tiers autorisés» ayant qualité pour les recevoir de façon ponctuelle et motivée (ex. : la police, le fisc).

La communication d'informations à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300 000 euros d'amende (article 226-22 du Code pénal).

Il est hors de question pour une entreprise de transmettre les données personnelles de ses utilisateurs ou clients à une entité tierce (effet relatif des conventions l'impose au même titre que le principe de confidentialité imposé par la loi de 1978).

Si un contrat de gestion des données devait être conclu avec un prestataire externe à l'entreprise, il conviendrait de lui faire assumer cette obligation de confidentialité et de bien préciser le périmètre de la mission qui l'autorise à gérer à son tour (en tant que co-responsable du traitement des données à caractère personnel) lesdites données.

La divulgation d'informations commise par imprudence ou négligence est punie de 3 ans d'emprisonnement et de 100 000 euros d'amende.

5. Le principe du respect du droit des personnes (obligation de transparence)

L'article 13 du RGPD dispose que :

« Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes :

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement

b) le cas échéant, les coordonnées du délégué à la protection des données;

c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement;

d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers;

e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent; et

f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, 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; »

Le responsable d'un fichier doit donc permettre aux personnes concernées par des informations qu'il détient d'exercer pleinement leurs droits. Pour cela, il doit leur communiquer : son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence de droits, les transmissions envisagées.

Le refus ou l'entrave au bon exercice des droits des personnes est puni de 1500 euros par infraction constatée et 3 000 euros en cas de récidive. (Article 110 du décret du 20 octobre 2005 et article 131-13 du Code pénal).

a) Informer les intéressés (article 13 du RGPD)

Lorsque les données sont recueillies par exemple par voie de questionnaire, les usagers concernés et le personnel de l'entreprise doivent être informés de la finalité du traitement du caractère obligatoire ou facultatif du recueil, des destinataires des données et des modalités d'exercice des droits qui leur sont ouverts au titre de la loi *« Informatique et Libertés »* : droit d'accès et de rectification mais aussi, droit de s'opposer, sous certaines conditions, à l'utilisation de leurs données.

L'article 15 du RGPD reconnait un droit pour la personne concernée par le traitement « de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement (...), ou du droit de s'opposer à ce traitement ».

b) Les droits d'accès et de rectification (article 39 de la loi informatique et libertés et

article 15 du RGPD)

Toute personne peut demander communication de toutes les informations la concernant contenues dans un fichier détenu par l'entreprise et a le droit de faire rectifier ou supprimer les informations erronées.

Toute personne peut demander la rectification des informations inexactes la concernant. Le droit de rectification complète le droit d'accès.
Il permet d'éviter qu'un organisme ne traite ou ne diffuse de fausses informations sur vous.

c) Le droit d'opposition ou de limitation du traitement (article 38 de la loi informatique et libertés et article 15 du RGPD)

Toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que des données la concernant soient enregistrées dans un fichier informatique, sauf si celui-ci présente un caractère obligatoire.

Vous pouvez donc vous opposer à ce que les données vous concernant soient diffusées, transmises ou conservées. Le droit d'opposition s'entend donc également comme un droit de suppression.

Focus sur le RGPD

Le Règlement n°2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après RGPD) a pour finalité de remplacer la directive 95/46/CE et instaurer un cadre général et unique pour la protection des données en Europe.

Sur proposition de la Commission européenne en date du 25 janvier 2012, ce Règlement a été adopté conjointement par le Parlement européen et le Conseil et est applicable depuis le 25 mai 2018.

Il convient d'abord de préciser que ce Règlement européen applicable depuis le 25 mai 2018, est, par essence, d'application directe dans tous les Etats membres de l'Union européenne, c'est à dire sans qu'il soit nécessaire d'attendre une quelconque transposition (à l'inverse de la Directive).

Une loi en date du 20 juin 2018 est venue modifiée la loi informatique et libertés de 1978 afin qu'elle mette en adéquation les dispositions du Règlement avec la loi française applicable tout en précisant des points pour lesquels le Règlement renvoie explicitement au Droit des Etats membres (notamment concernant les données sensibles).

- **Un texte qui harmonise les législations européennes en matière de respect des données à caractère personnel**

Parce que la précédente règlementation[1] (issue d'une Directive en date du 24 octobre 1995) n'était plus adaptée aux enjeux économiques et juridiques liés à l'exploitation des données personnelles par les acteurs du monde du numérique, parce qu'il convenait qu'un texte vienne durcir les contraintes et sanctions en la matière et surtout parce que ce texte imposera aux Etats membres de l'Union européenne des dispositions communes en vue de remplacer les règlementations nationales qui présentent actuellement des disparités significatives, la promulgation du Règlement général sur la protection des données **(ci-après le « RGPD » ou le «Règlement »)**[2] devenait une nécessité.

- **Un texte avec un champ d'application dépassant les frontières de l'Union européenne**

Le RGPD a vocation à s'appliquer aux traitements de données à caractère personnel qui ont lieu sur le territoire de l'Union Européenne, à ceux qui touchent des ressortissants européens (même lorsque le traitement a lieu hors UE), mais aussi à ceux pour qui le responsable de

[1] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

[2] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

traitement (i.e. « data controller ») et/ou le sous-traitant (i.e. « data processor ») sont établis sur le territoire de l'Union européenne.

- **Un texte applicable depuis le 25 mai 2018**

Si le RGPD est entré en vigueur le 27 avril 2016, sa mise en application est effective depuis le 25 mai 2018. Les entreprises devront, au plus tard à cette date, être en conformité avec le Règlement. Celle qui sont l'objet de poursuite pour des faits constatés avant cette date se verront sanctionnées sur la base de l'ancienne règlementation sur la base du principe d'application de la loi dans le temps.

- **Un texte visant à une meilleure protection des personnes concernées**

L'objectif principal du RGPD est d'assurer une meilleure protection des personnes concernées par les traitements de données à caractère personnel ainsi que la sécurité, l'intégrité, la confidentialité et la nécessité desdits traitements et de l'utilisation des données à caractère personnel.

En conséquence, le Règlement vient, de façon générale, renforcer certaines dispositions qui existent déjà, notamment, au niveau de la législation française via la loi informatique et libertés du 6 janvier 1978 modifiée, créer de nouvelles obligations pour le responsable du traitement (i.e. la personne physique ou morale qui détermine les finalités et les moyens de toute opération appliquée à des données à caractère personnel et pour le compte de laquelle est réalisée le traitement) tout comme pour les sous-traitants (i.e. les personnes qui traitent les données à caractère personnel uniquement pour le compte et sur les instructions du responsable de traitement) et enfin changer la manière dont les différents acteurs doivent appréhender leur politique en matière de traitement et gestion des données à caractère personnel pour se conformer aux exigences règlementaires.

- **Une mise à jour significative et ambitieuse du barème des sanctions**

L'une des raisons pour lesquelles le RGPD fait tant parler tient au fait qu'il prévoit des amendes maximales, pour non-respect des dispositions légales, qui dépassent largement les standards actuels en vigueur en France, même si les sanctions, qui étaient jusqu'il y a peu de temps assez faibles, (jusqu'à 150 000 euros d'amende) ont été revues à la hausse depuis la loi pour la République Numérique du 7 octobre 2016 (jusqu'à 3 millions d'euros).

Ceux qui contreviendront au RGPD s'exposeront à des amendes qui pourront varier en fonction du type d'infraction. Elles pourront s'élever jusqu'à 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé pouvant être retenu (*exemples : absence de protection des données dès la conception, non-respect de la désignation d'un DPD)* voire selon un autre type d'infraction jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé pouvant être retenu (exemples : *infraction relative aux transferts des données ou aux non-respect des règles du consentement au traitement*).

Ces sanctions sont désormais susceptibles de faire peur aussi bien aux grandes entreprises qu'aux PME/TPE, et ce d'autant plus que depuis la loi pour une république numérique du 7 octobre 2016, il est possible, en France, de sanctionner les entreprises sans mise en demeure préalable quand le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la CNIL pourra prononcer directement des sanctions pécuniaires (article 65).

- **Des obligations étendues et des droits renforcés**

Le RGPD renforce le droit des personnes à travers les notions, déjà existantes en France, d'accès, de rectification et d'opposition tout en créant un droit de suppression renforcé, qualifié de droit à l'oubli, opposable au responsable du traitement notamment quand les données ne sont plus nécessaires au regard de la finalité pour lesquelles elles ont été collectées ainsi que d'un droit à la portabilité (au sens d'une disposition visant à permettre aux personnes de récupérer les données personnelles les concernant qu'elles avaient, elles-mêmes, transmises au responsable du traitement).

Le RGPD impose, à l'instar de la loi informatique et libertés de 1978 modifiée, que le respect des droits des personnes passe par le fait pour le responsable du traitement de s'assurer que le traitement qu'il met en œuvre soit **licite**, (au sens où il doit être soit consenti par la personne concernée, soit nécessaire à l'exécution du contrat signé par cette personne, soit découler du respect d'une obligation légale, soit d'un intérêt légitime du responsable du travail du traitement qui ne devra pas être inférieur aux intérêts de la personne concernée).

Il devra également vérifier que le traitement est **loyal**. Ainsi, seules les données adéquates, nécessaires et pertinentes devront être collectées et ce selon des finalités déterminées, explicites et légitimes (transposition du principe de proportionnalité présent dans la loi informatique et libertés de 1978 modifiée).

Le responsable du traitement devra **obtenir un consentement de la personne concernée** lequel se devra d'être « *un acte positif clair par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des données à caractère personnel la concernant* ».

Cette exigence interdit de considérer le silence ou l'absence d'opposition (au sens d'une inaction) comme un consentement univoque et oblige les responsables de traitement à recueillir et conserver les éléments de preuve démontrant l'acte positif manifestant le consentement aussi bien sous forme électronique, par voie orale, par écrit ou par tout autre moyen. (ex : une case à cocher sur un site web accompagnée d'un texte manifestant ce consentement libre et éclairé).

La question de la durée du traitement est également abordée par le RGPD. Il prévoit que les données des personnes ne doivent être conservées que pour la durée strictement nécessaire au but poursuivi par le responsable du traitement. Dès lors, à l'issue de ce délai, le responsable du traitement devra s'assurer que les données soient détruites ou anonymisées, de sorte, dans le second cas évoqué, qu'il soit impossible d'associer cette donnée à une personne déterminée.

- **Quid des transferts de données hors de l'Union européenne ?**

Le RGPD reprend en substance la règlementation actuelle s'agissant de l'encadrement des transferts de données à caractère personnel hors de l'Union Européenne et de l'Espace Economique Européen.

Lesdits transferts seront autorisés à la condition d'être fondés, sur une décision d'adéquation, sur des garanties appropriées, qu'ils prennent la forme de règles d'entreprise contraignantes, ou qu'ils résultent de situations particulières (clauses contractuelles types dites CCT ou BCR Binding corporate rules / règles contraignantes d'entreprises).

Les Clauses Contractuelles Types sont des modèles de contrats de transfert de données personnelles adoptés par la Commission européenne.

Les Binding Corporate Rules (BCR) désignent une politique de protection des données intra-groupe en matière de transferts de données personnelles hors de l'Union européenne. Elles sont juridiquement contraignantes et respectées par les entités signataires du groupe, quel que soit leur pays d'implantation, ainsi que par tous leurs salariés d'une même entreprise ou d'un même groupe.

La différence majeure avec le cadre juridique actuel tient essentiellement dans le fait qu'à terme, les pays étant considérés comme assurant un niveau de protection adéquat (i.e. les pays situés hors du territoire de l'Union Européen mais pour lesquels les transferts de données à caractère personnel étaient autorisés) ne seront plus fixés individuellement par les Etats-Membres, mais par la Commission européenne.

Nous allons aborder successivement la question du passage d'un système de formalités préalables au traitement au principe d'accountability (I), le développement des exigences liées à la sécurité des données inhérent au RGPD (II) et enfin l'obligation de désigner un Délégué à la protection des données (ci-après « DPD » ou « Data protection officer - DPO ») (III).

I. Un changement par rapport à la politique de traitement des données à caractère personnel actuellement en vigueur

Le RGPD instaure une nouvelle façon d'aborder les obligations relatives au traitement des données à caractère personnel par le responsable dudit traitement.

A. Un changement de paradigme

Ce changement que met en œuvre le RGPD tient notamment au fait qu'il supprime (mis à part quelques cas spécifiques) l'exigence de déclarations préalables au traitement (déclaration simplifiée, normale, demande d'avis, demande d'autorisation préalable) en faisant désormais peser sur le responsable du traitement la responsabilité de mettre en place les mesures techniques et fonctionnelles appropriées afin d'être en conformité avec le RGPD.

Il peut s'agir notamment de la mise en place de politique interne de gestion des données à caractère personnel, de mesures liées aux outils informatiques qui traitent ces données, ainsi que de mesures de traçabilité visant à démontrer à l'autorité nationale qu'elles ont bel et bien été mises en œuvre.

En tout état de cause, le responsable de traitement ainsi que le sous-traitant des traitements de données à caractère personnel devront tenir un registre de traitements indiquant à minima la finalité du traitement, les mesures mises en œuvre pour assurer la sécurité, la confidentialité et l'intégrité des données à caractère personnel, la durée de conservation des données à caractère personnel ainsi que les personnes ayant accès auxdites données et le tenir à la disposition de la CNIL en cas de contrôle (article 30 du RGPD).

L'article 30 du RGPD qui dispose que :

> *« Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:*
> *a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;*
> *b) les finalités du traitement;*
> *c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;*
> *d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;*
> *e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa, les documents attestant de l'existence de garanties appropriées;*
> *f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;*
> *g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles visées à l'article 32, paragraphe 1 ».*

Ces registres répondent donc notamment aux questions suivantes :

- QUI ? (Le nom et les coordonnées du responsable du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données ; Catégories de données traitées
- POURQUOI ? La ou les finalités pour lesquelles sont collectées ou traitées ces données
- OÙ ? Lieu où les données sont hébergées. Dans quels pays les données sont éventuellement transférées.
- JUSQU'À QUAND ? Pour chaque catégorie des données, combien de temps sont-t-elles conservées.

- COMMENT ? Quelles mesures de sécurité sont mises en œuvre pour minimiser les risques.

B. Privacy by design / privacy by default

C'est ce même principe d'accountability ou de « responsabilisation » qui implique que le responsable du traitement comme le sous-traitant soient tenus, dès la conception des produits et services, de mettre en œuvre un socle protecteur des données à caractère personnel (notion dite de « ***privacy by design »***).

De la même façon, ils devront s'assurer que sans l'intervention préalable des personnes physiques concernées, les données à caractère personnel ne peuvent être rendues accessibles à un nombre indéterminé de personnes physiques et, que soient collectées et traitées uniquement des données à caractère personnel pertinentes au regard de la finalité du traitement considéré (notion dite de « ***privacy by default »*** (article 25 § 2).

le Privacy by design (sécurité dès la conception) consiste donc à mettre en œuvre, dès la conception des produits et services, un socle protecteur des données à caractère personnel. Cela signifie par exemple que le concepteur du logiciel devra avoir pensé au respect des données à caractère personnel dès la conception dudit produit afin de ne pas mettre en difficulté l'utilisateur (client).

Le Privacy by default (sécurité par défaut) consiste quant à lui au fait de restreindre l'accès aux données personnelles à des personnes déterminées et ne collecter que les données pertinentes au regard de la finalité du traitement. Il faut que dans l'utilisation du logiciel, le responsable du traitement s'assure que seules les personnes habilitées par leurs fonctions à avoir accès à une donnée puissent y avoir accès (authentification/droit d'accès/habilitation).

II. D'importantes attentes en matière de sécurité

Le responsable du traitement ainsi que son sous-traitant sont tenus de mettre en œuvre des mesures de sécurité appropriées aux données qu'ils collectent.

L'article 32.1 du RGPD dispose que : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins: a) la pseudonymisation et le chiffrement des données à caractère personnel; b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement; c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique; d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* ».

L'article 32.2 précise que : « *Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite* ».

Il existe un caractère subjectif réel dans l'appréciation que vous ferez des mesures de sécurité à mettre en oeuvre conformément à l'article 32 du RGPD (nature des données traitées, sensibilité de la donnée, domaine d'activité du responsable de traitement, état de l'art en matière de sécurité, mesures jugées élémentaires, etc..).

Parmi les quelques mesures qu'il est possible de citer comme élémentaires :

- que les supports sur lesquels reposent les traitements de données à caractère personnel ont été recensés.
- que des mesures de sécurité (physique) sont mises en œuvre pour empêcher que les données à caractère personnel soient déformées, endommagées ou que des tiers non autorisés y aient accès.
- que les systèmes installés peuvent être rétablis en cas d'interruption
- que les fonctions du système opèrent, que les erreurs de fonctionnement soient signalées (fiabilité) et que les données à caractère personnel conservées ne puissent pas être corrompues par un dysfonctionnement du système (intégrité). ;
- la définition d'un identifiant unique par utilisateur salarié du SI et interdit les comptes partagés entre plusieurs d'entre eux (même si quelques comptes partagés subsistent)
- que la recommandation de la CNIL concernant les mots de passe est respectée
- supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou à une ressource informatique, ainsi qu'à la fin de leur contrat
- utiliser des logiciels régulièrement mis à jour
- Imposer l'utilisation d'un VPN pour l'accès au réseau local à distance (hors du lieu de travail)
- utiliser pour le réseau Wifi un chiffrement conforme à l'état de l'art (WPA 2, WPA2 PSK)

Tout ou partie des questions visant à évaluer le niveau de sécurité des données personnelles peuvent se trouver dans le guide de la CNIL – édition 2018 intitulé « sécurité des données personnelles ».

Sur ce point, le RGPD a créé l'exigence d'analyse d'impact (A) ainsi que l'obligation de notification des failles de sécurité (B) et contribue à une plus grande responsabilisation des sous-traitants vis-à-vis des responsables du traitement (C).

A. L'avènement de l'analyse d'impact

La contrepartie de cette liberté offerte par l'accountability tient au fait de mettre désormais à la charge du responsable du traitement ou du sous-traitant le soin de réaliser une analyse

d'impact que l'on peut définir comme une évaluation interne des risques d'atteinte à la vie privée des personnes concernées que certains traitements de données à caractère personnel peuvent faire encourir.

Il conviendra donc que les entreprises procèdent à un audit préalable afin de vérifier si elles sont susceptibles, compte tenu de leur activité, de la nature des données ou du traitement de données à caractère personnel envisagé, de faire courir un risque « élevé » d'atteinte à la vie privée des personnes concernées par ledit traitement et donc de déterminer si l'analyse d'impact doit ou non être réalisée.

B. L'obligation de notifier les violations de données personnelles

Jusqu'ici, seuls les fournisseurs de communication électronique avaient pour obligation de notifier à la CNIL (Commission Nationale de l'Informatique et des Libertés) les violations de données personnelles qu'ils avaient subies.

Le RGPD a le mérite de généraliser cette obligation de notification de violation de données personnelles, dans un délai de 72 heures à compter de la connaissance de cette violation, à l'autorité nationale de contrôle (CNIL en France), laquelle s'impose désormais à tout responsable de traitement ayant eu à subir une faille de sécurité, au sens d'une intrusion ayant entrainé la destruction, la perte, l'altération, ou l'accès non autorisé à des données personnelles, hormis quand il est en mesure de démontrer qu'il n'existe aucun risque pour les personnes (exemple : faille impliquant des données chiffrées et/ou anonymisées).

Par ailleurs, quand il existe un risque grave pour les personnes physiques concernées par la faille, le responsable du traitement se doit de les avertir personnellement de l'existence dudit risque, en plus des démarches initiées auprès de l'autorité nationale de contrôle.

Ladite notification devra d'ailleurs contenir :

- une description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- la communication du nom et des coordonnées du Délégué à la Protection des Données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- une description des conséquences probables de la violation de données à caractère personnel ;
- une description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Une Politique de gestion des failles de sécurité devra être établie et devra prévoir l'investigation de la faille et l'apport des correctifs nécessaires. Le tout devra être documenté selon un process similaire aux éléments figurant ci-dessous.

A chaque fois qu'une faille de sécurité sera établie, une analyse devra être faite afin de déterminer si cette faille constitue ou non une violation de données personnelles au sens du RGPD.

Dans l'affirmative, l'entreprise déterminera s'il est nécessaire d'informer la CNIL, d'une part, et les personnes concernées, d'autre part.

Pour qu'il y ait violation, 2 conditions cumulatives doivent être réunies à savoir la mise en œuvre d'un traitement de données personnelles (1) et que ces données aient fait l'objet d'une violation (2) (perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite).

Dans le cadre de la procédure de gestion des failles de sécurité mise en place, il doit être prévu de documenter systématiquement en interne l'incident en déterminant :

- La nature de la violation si possible
- Les catégories et le nombre approximatif de personnes concernées par la violation les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés

Il doit être prévu de décrire :

- Les conséquences probables de la violation de données ;
- Les mesures prises ou envisagées pour éviter que cet incident se reproduise ou atténuer les éventuelles conséquences négatives.

Si l'incident constitue un risque au regard de la vie privée des personnes concernées, il est notifié à la CNIL.

En cas de risque élevé, il est prévu d'informer également les personnes concernées. En cas de doute, il faudra le notifier à la CNIL qui déterminera ensuite s'il est nécessaire ou non d'informer les personnes.

La notification doit être transmise à la CNIL dans les meilleurs délais à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes.

En cas d'investigation, une notification en deux temps est possible :

- Une notification initiale dans les meilleurs délais à la suite de la constatation de la violation
- Puis, une notification complémentaire dans le délai de 72 heures si possible après la notification initiale. Si le délai de 72 heures est dépassé, il conviendra d'expliquer, lors de votre notification, les motifs du retard.

C. Une plus grande responsabilisation des sous-traitants vis-à-vis des responsables du traitement

Le RGPD consacre la possibilité d'un partage de responsabilités du traitement entre le responsable du traitement et le sous-traitant, mais précise surtout qu'il est attendu du responsable du traitement une obligation de vigilance quant au choix des sous-traitants.

On attend de lui qu'il s'assure que son sous-traitant présente des garanties de protection suffisantes dans le traitement des données personnelles.

Cela passera notamment par le fait de formaliser un contrat de sous-traitance dans lequel le sous-traitant attestera avoir mis en œuvre un certain nombre de mesures de sécurité élémentaires et en rapport direct avec la sensibilité et la quantité des données qu'il traite pour le compte du responsable du traitement et, principale innovation du RGPD, dans lequel seront décrites les obligations et les responsabilités inhérentes au responsable de traitement et au sous-traitant.

Nous sommes encore aujourd'hui dans l'attente des précisions de la Commission Européenne s'agissant du partage des obligations et des responsabilités et notamment de modèles types de clauses pour encadrer les responsabilités du responsable de traitement et du sous-traitant.

Le sous-traitant devra, par ailleurs, veiller à informer le responsable du traitement des failles qu'il aurait subies afin que le responsable du traitement puisse ensuite respecter l'obligation de notification à laquelle il est personnellement tenu.

III. La désignation obligatoire d'un Délégué à la Protection des Données (ci-après « DPD » - traduction française de Data Protection Officer ou « DPO »)

Parce que le principe d'accountability consiste en quelque sorte en un contrat de confiance entre l'autorité nationale de contrôle et les acteurs traitant de ces données que sont le responsable du traitement et son sous-traitant, le RGPD a voulu que certaines personnes, soit parce qu'elles sont une autorité publique ou un organisme public, soit parce qu'elles proposent un suivi régulier et systématique à grande échelle de données personnelles, soit parce qu'elles traitent des catégories particulières de données personnelles (parmi lesquelles les données sensibles), se voient dans l'obligation de désigner un DPD (ou DPO en anglais).

A l'instar du Correspondant Informatique et Libertés (CIL), le DPD peut être un salarié ou un intervenant extérieur de l'entreprise (avocat, consultant) à la condition qu'il présente des compétences juridiques suffisantes et que son indépendance soit garantie.

Ce délégué aura pour mission d'informer, de former et de conseiller le responsable du traitement ou le sous-traitant.
Il devra, par ailleurs, contrôler le respect du RGPD européen et de la loi nationale. Enfin, il coopérera avec l'autorité de contrôle et sera ainsi le point de contact de celle-ci.

Il est donc vivement conseillé à l'entreprise qui se verra dans l'obligation de désigner un DPD à compter du 25 mai 2018, de réfléchir, dès à présent, à la nomination d'un tel profil, qualifié d'abord de CIL et à terme DPD, afin que la mise en place de mesures visées dans le RGPD, au-delà même de sa simple nomination, soit envisagée et supervisée bien en amont de la date de mise en application du RGPD.

CONCLUSION

Ce tour d'horizon des avancées et des nouveautés issues du RGPD mérite que les sociétés s'y attardent et qu'elles se fassent conseiller dans la mise en œuvre des mesures qui seront attendues d'elles, eu égard aux risques accrus de sanctions (jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent ou 20 millions d'euros d'amende).

Il est donc essentiel qu'elles s'y préparent avec l'aide de leurs propres services juridiques, pour celles qui en ont les moyens, ou de prestataires extérieurs parmi lesquels les cabinets d'avocats intervenant en la matière.

Gageons que les moyens humains et financiers mis en œuvre ainsi que le temps qu'elles auront consacré en vue d'une mise en conformité complète de leurs systèmes d'information avec le RGPD seront autant d'éléments pris en compte par l'Autorité nationale de contrôle.

Une mise en conformité en bonne et due forme passe par :

- **un audit des pratiques du Client par recensement des informations ;**
- **l'élaboration d'un rapport d'audit identifiant les non conformités, d'une part, et faisant état des préconisations et des propositions d'actions, d'autre part ;**
- **une régularisation de ce qui d'un point de vue juridique peut l'être ce qui exclut de fait les prestations techniques qui seront sous-traitées à un tiers partenaire ou celui dont le Client fera savoir qu'il souhaite le solliciter pour ses compétences ou pour son expérience du système d'information du Client.**