De quoi le RGPD est-il le nom ?

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 impose 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 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 24 mai 2016, sa mise en application date du 25 mai 2018. Les entreprises devaient, au plus tard à cette date, être en conformité avec le Règlement. Celles 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.

[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

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.

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.

Outre les éléments évoqués précédemment, le présent Livre Blanc abordera d'autres points importants du RGPD, mais ne pourra prétendre, compte tenu de sa taille, à l'exhaustivité.

Nous allons donc 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).

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).

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.
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.

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 passe 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.

Les Avocats du site RGPD.co sont disponibles et compétents pour remplir ce type de mission pour le compte du Client en tant que DPD externe.

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.

Les Avocats de RGPD.co sont disponibles pour répondre à toutes vos interrogations en la matière.

Dans une optique de mise en conformité de la société qui les sollicitera avec les exigences figurant dans le RGPD, ils procèderont successivement à :

- **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.**

Ils sont également disponibles dans l'hypothèse d'un accompagnement au titre d'une mission de Délégué à la protection des données externe.

Sadry PORLON
Avocats au Barreau de Paris

Cabinet Sadry Porlon
38 avenue Hoche - Paris 75008
Tél. : 01 77 45 52 96
Fax : 09 72 16 37 15