INTRODUCTION

- Le développement considérable et la rapidité d'échange des flux d'information via les réseaux informatiques et les objets connectés peuvent constituer un risque important pour les citoyens au regard de leurs droits et de leurs libertés en particulier en matière de respect de la vie privée (utilisation abusive du e-marketing, e-réputation, risques de fraudes bancaires, usurpation d'identité, etc.…).
- Face à ce bouleversement numérique, les institutions européennes ont souhaité voir appliquer un cadre juridique plus contraignant permettant une meilleure protection des données à caractère personnel et une maîtrise plus importante par les citoyens de leurs données.
- La question du traitement des données personnelles est, en France, régit principalement par la loi informatique et libertés du 6 janvier 1978, telle que modifiée par la loi du 6 août 2004.
- Jusqu'à maintenant, était institué un système de déclaration ou d'autorisation de fichiers de données personnelles.
- Le Règlement 2016/679 du parlement Européen et du Conseil en date 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 (RGPD), vient modifier largement les dispositions applicables en renforçant les droits des personnes et en créant une obligation de sécurisation pour les responsables de traitement de données.
- Ce règlement oblige, par ailleurs, les responsables de traitement de données à caractère personnel à la mise en place d'une documentation juridique permettant de justifier le respect des dispositions du règlement auprès de l'autorité de contrôle, à savoir la CNIL.
- Le règlement sera applicable le 25 mai 2018. Il est assorti de lourdes sanctions en cas de manquement.
- D'ores et déjà, il appartient aux responsables de traitement, à savoir les entreprises du secteur privé et du secteur public ainsi que les organismes de droit public (collectivités territoriales, administration…) de mettre en place une organisation et une documentation permettant de démontrer le respect des dispositions du RGPD.
- Cette conformité au RGPD permettra ainsi, outre le fait d'éviter de lourdes sanctions financières, d'instaurer une confiance entre les entreprises et administrations et les personnes concernées (clients, administrés). Elle pourra également permettre, le cas échéant, aux entreprises et aux administrations de bénéficier d'un Label Gouvernance délivré par la CNIL.

1 Qui est concerné ?

Le nouveau Règlement européen sur la protection des données à caractère personnel s'applique à tout traitement de données à caractère personnel mis en œuvre dans le cadre de l'activité d'un établissement.

Le Règlement ne s'applique pas à une personne physique dans le cadre d'une activité strictement personnelle ou domestique.

Il s'applique, en outre, que le traitement soit informatique ou sur support papier.

Ainsi, toute entreprise du secteur privé ou du secteur public et toutes entités administratives ayant constitué un fichier de personnes physiques doit respecter le RGPD.

Seul est visé le fichier de personnes physiques. Un fichier de personnes morales (sociétés) n'est pas visé.

Les administrations opérant dans le domaine de la prévention et de la détection des infractions pénales ou des menaces à la sécurité publique ne sont pas concernées par le RGPD.

Le nombre de professionnels concerné est donc considérable. Il pourra s'agir, à titre d'exemple des entreprises sur Internet vendant leurs produits ou leurs services à des clients particuliers, des sociétés de vente par correspondance, des réseaux de franchise, des cliniques, hôpitaux, EDF, agences immobilières mais aussi des collectivités locales, les sociétés de sécurité, de transport, etc.…

2 Application territoriale du Règlement

Face à la puissance de certaines entreprises étrangères, en particulier américaines (Facebook, Amazon, Google…), les institutions européennes ont souhaité que le RGPD leur soit également applicable.

Ainsi, dès lors qu'une entreprise, même non installée sur le territoire d'un Etat membre de l'Union Européenne, met en œuvre un traitement de fichiers de personnes physiques relatif à des citoyens d'un pays membre de l'Union Européenne, dans le cadre de son offre de biens ou services, elle est assujettie au RGPD.

Concrètement, cela signifiera qu'une entreprise non européenne devra désigner un représentant au sein de l'Union Européenne, la plupart du temps un délégué à la protection des données, afin de la représenter.

3 Démontrer à la CNIL sa conformité aux obligations de protection des données personnelles

Le chef d'entreprise ou le responsable d'une Administration ou d'une collectivité territoriale qui a connaissance d'un fichier de personnes physiques, faisant l'objet d'un traitement, au sein de son établissement, doit mettre en œuvre les mesures adéquates pour respecter le RGPD.

Faute par lui de prendre ces mesures, il expose son entreprise ou son Administration au paiement d'une très forte amende (20 millions d'euros ou 4% de son chiffre d'affaires).

Concrètement, comment le responsable d'un traitement doit-il procéder pour respecter le RGPD ?

La première chose à faire est de s'entourer de conseils en informatique et en droit. Idéalement, il conviendra de désigner un délégué à la protection des données qui pourra agir en tant que chef d'orchestre dans la mise en œuvre du RGPD et de lien avec la CNIL.

Par suite, le responsable du traitement devra établir un état des lieux, une cartographie de l'état des traitements de données à caractère personnel avant de mettre sur pied une politique de protection de ces données formalisée par une charte écrite décrivant l'ensemble du processus de protection.

[A] Réaliser une cartographie des traitements et une étude d'impact sur la vie privée

Pour mesurer l'impact du Règlement sur la protection des données de l'activité d'une entreprise ou d'une administration, il convient, dans un premier temps, de recenser de façon précise les traitements de données mis en œuvre.

Pour cela, il conviendra de détailler :
- les différents traitements,
- les catégories de personnes traitées,
- les objectifs poursuivis par les opérations de traitements,
- les personnes en interne ou en externe qui traitent ces données ainsi que les sous-traitants,
- les flux en indiquant l'origine et la destination des données,
- les éventuels transferts dans et en dehors de l'Union Européenne,
- le lieu d'hébergement des données,
- le temps de conservation des données,
- la description des mesures de sécurité mises en œuvre pour minimiser les risques d'accès non autorisés aux données,
- l'impact sur la vie privée des personnes concernées.

Une fois ce travail de cartographie effectué, il conviendra de dresser un registre des traitements avec un tableau synthétique détaillant les informations ci-dessus.

Si l'entreprise ou l'Administration a identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, il conviendra de mener une étude d'impact sur la protection des données.

Ainsi, il faudra procéder à une description du traitement et de ses finalités. Evaluer la nécessité et la proportionnalité du traitement, apprécier les risques sur les droits et les libertés des personnes concernées.

Il est, en effet, rappelé que le Règlement précise que le traitement doit être effectué de manière licite, loyale et transparente. Cela signifie que les données collectées doivent être strictement nécessaires à la finalité du traitement. Il convient de ne pas collecter plus d'information que nécessaire par rapport à l'objectif et à l'activité de l'entreprise.

Les données doivent également être mises à jour régulièrement afin d'être exactes.

[B] Mettre en place des mesures permettant la protection des données dès leur conception (*Privacy by design*) et par défaut (*Privacy by default*)

Auparavant, les entreprises ou les administrations avaient pour seule obligation celle de déclarer un traitement de données ou d'être autorisées à le détenir pour les activités les plus sensibles, auprès de la CNIL.

À partir du 25 mai 2018, ces obligations n'existeront plus.

Les acteurs devront mettre en place, dès la conception du traitement et du fichier, des mesures permettant la protection des données et qui pourront prendre les formes suivantes :

- pseudonymisation,
- minimisation des données,
- chiffrement,
- éloignement des sources de risques,
- obligation de notification des failles de sécurité,
- accréditation spéciale de certaines personnes pour traiter les données,
- autorisation spéciale pour effectuer un transfert,
- détail des contrats passés avec les sous-traitants,
- politique d'archivage et de conservation des données,
- formation périodique des salariés,
- désignation d'un délégué à la protection des données.

[C] – Mise en place d'un registre des traitements et d'une charte de sécurisation des données :

Face à ces nouvelles obligations en matière de protection des données, la CNIL sera habilitée à constater leur respect ou leur manquement.

Il conviendra, dès lors, de pouvoir démontrer à la CNIL que l'entreprise ou l'Administration répond aux exigences du Règlement.

Cette démonstration sera effectuée, dans un premier temps, par la tenue d'un registre de traitements détaillant les catégories et les objectifs du traitement considéré. La tenue de ce registre sera obligatoire pour les entreprises de plus de 250 salariés.

L'entreprise ou l'administration devra également établir une charte écrite détaillant sa politique et les mesures qu'elle a mise en œuvre pour protéger les données à caractère personnel.

Là encore, la désignation d'un délégué à la protection des données, qui aura pu être en lien direct avec la CNIL, paraît incontournable.

4 Le renforcement des droits des personnes concernées

Le RGPD oblige les entreprises et les administrations à prendre des mesures visant à protéger les données à caractère personnel.

Il oblige également les entreprises et les administrations à améliorer le consentement de la personne physique concernée et crée de nouveaux droits au bénéfice de cette dernière.

[A] – Le renforcement du consentement de la personne concernée

La personne concernée doit donner son accord avant que le responsable puisse procéder au traitement de ses données personnelles.

Dans certaines hypothèses, l'obtention du consentement n'est pas nécessaire. Essentiellement lorsque le responsable du traitement invoque un « intérêt légitime » ou lorsqu'il doit répondre à une obligation légale. On imagine ici une Administration ou une collectivité territoriale dont les obligations législatives requièrent l'obtention d'un certain nombre de données de ses administrés.

Lorsque le consentement est requis, il appartient au responsable du traitement de prouver que le consentement a été donné et il est désormais prévu que la personne concernée puisse retirer ce consentement.

Par ailleurs, le consentement ne peut avoir été donné passivement. Il faut un acte clair et positif de la personne concernée. Ainsi, par exemple, la personne concernée devra donner son consentement en cochant une case spécifique et indépendante.

Une hypothèse particulière est prévue par le règlement lorsqu'un enfant doit donner son consentement. Le texte prévoit que le consentement de l'enfant (âge à définir par les Etats membres entre 13 et 16 ans) doit être donné par la personne ayant l'autorité parentale.

[B] – Les nouveaux droits des personnes concernées

Les personnes concernées disposaient déjà de droits au titre de la législation actuelle. Il s'agit des droits d'accès, d'opposition et de déréférencement au traitement de données.

Le RGPD crée de nouveaux droits :
- le droit à l'oubli,
- le droit à la limitation du traitement,
- le droit de s'opposer au profilage (*le profilage est défini comme le fait d'analyser et de prédire les comportements futurs d'une personne*),
- le droit à la portabilité des données : l'exercice de ce droit permettra aux personnes de récupérer les données personnelles qu'elles ont communiquées par exemple en les téléchargeant. Elles pourront également demander à un responsable de traitement de transférer directement ses données à un autre responsable de traitement.

Ces nouveaux droits devront être portés à la connaissance des personnes concernées.

[C] – L'adaptation des clauses d'un site internet ou des conditions générales de vente ou de prestation de service

La nécessité de recueillir le consentement positif et sans équivoque de la personne concernée et d'informer cette dernière de ses droits exigeront du responsable du traitement de modifier ses conditions générales ou l'organigramme de son site Internet.

5 Le Délégué à la Protection des Données (DPO)

Le RGPD crée une nouvelle fonction : Le Délégué à la protection des données (DPO).

La désignation d'un DPO sera obligatoire lorsque le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions, ou lorsque les activités de base de l'entreprise (privée ou publique) consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées.

Pour les autres entités, la désignation d'un DPO est facultative.

Dès lors, comment savoir si l'organisme ou l'entreprise doit désigner un DPO ?

Pour les autorités et les organismes publics, il ne fait aucun doute, la désignation d'un DPO est obligatoire.

Pour les sociétés du secteur privé, cette désignation est également obligatoire lorsque son activité principale consiste justement à traiter des données à caractère personnel.

À titre d'exemple, une société de surveillance chargée d'assurer la sécurité de lieux publics ou de centres commerciaux.

Il pourra également s'agir de clinique ou d'hôpitaux qui recueillent d'importantes données personnelles ou encore d'applications sur Smartphone dédiées au sport et dans le cadre desquelles les personnes concernées rentrent leurs données.

En tout état de cause, pour les institutions européennes, la désignation d'un DPO se veut la plus large possible.

[A] Quelles seront les missions du DPO ?

Le DPO sera le garant de la conformité à la nouvelle réglementation en matière de protection des données.

Rapportant directement au chef d'entreprise ou au chef d'établissement administratif, le DPO aura pour mission de conseiller l'entreprise, contrôler le respect du droit des données, coopérer et faire office de point de contact avec la CNIL.

Il pourra également assurer la formation de certains salariés sur les problématiques de protection des données.

Enfin, ses coordonnées pourront figurer sur le site internet de l'entreprise ou de l'Administration à destination des personnes concernées, à charge pour lui de répondre aux questions de ces dernières.

[B] Qui désigner en qualité de DPO ?

Le DPO pourra être un salarié de l'entreprise ou une personne externe à l'entreprise, tel qu'un avocat ou un conseil en informatique justifiant de solides connaissances juridiques en matière de protection des données et de libertés publiques. Pour des questions d'indépendance, il est néanmoins préférable de désigner un intervenant extérieur.

6 Les transferts de données personnelles

Le RGPD encadre les transferts de données à caractère personnel d'un pays membre de l'Union Européenne vers un pays tiers.

Les transferts vers certains pays ne nécessiteront pas d'autorisation spécifique ou d'accord particulier. Tel sera le cas de pays dont le niveau de protection est considéré comme similaire à l'Union Européenne (Norvège, Canada, Suisse, Nouvelle-Zélande…).

Pour d'autres pays, le transfert sera soumis à un cadre juridique plus spécifique.

7 Le renforcement des obligations des sous-traitants

Le sous-traitant est celui qui traite les données à caractère personnel pour le compte de celui (entreprise, administration…) qui est responsable du traitement.

Le RGPD indique qu'il devra présenter des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles permettant au traitement de répondre aux exigences du RGPD.

Par ailleurs, le RGPD instaure de nouvelles obligations pour le sous-traitant dont les contours devront se retrouver dans le contrat de sous-traitance, à savoir :
- l'objet et la durée du traitement,
- la nature et la finalité du traitement,
- les obligations de sécurité, d'avertissement et d'alerte envers le responsable du traitement.

S'il outrepasse ses fonctions, ou n'agit pas selon les instructions du responsable du traitement, il pourra engager sa responsabilité.

8 Les sanctions financières

En cas de manquement, le responsable du traitement peut être condamné au paiement d'une amende de 20 millions d'euros ou de 4 % de son chiffre d'affaires.

Les sanctions financières sont donc extrêmement dissuasives. Elles visent, naturellement, en premier lieu les grands acteurs de l'Internet (Amazon, Facebook…).

Néanmoins, face aux risques d'atteinte à la vie privée, la CNIL aura vocation à contrôler tout responsable de traitement.

Ainsi, il appartient à chaque entreprise, chaque administration de respecter scrupuleusement le dispositif du Règlement, sans penser qu'elle ne pourra pas être dans le viseur de la CNIL.

9 Le label Gouvernance CNIL

Le RGPD prévoit la possibilité de mettre en place un système de certification en matière de protection des données.

La CNIL parle de Label Gouvernance.

Il est recommandé aux entreprises disposant d'un DPO d'obtenir ce label.

Il permettra ainsi d'accroître la confiance des clients ou des administrés dans l'entité gérant leurs données personnelles et pourra constituer un avantage concurrentiel.

EN RÉSUMÉ

D'un point de vue juridique, les entreprises et les administrations devront :

- désigner un DPO,
- procéder à un état des lieux (cartographie) de leurs traitements de données à caractère personnel,
- mettre en place un registre des traitements,
- rédiger une charte de la politique de protection des données personnelles,
- modifier ses conditions générales de façon à obtenir le consentement de la personne concernée et lui rappeler ses droits,
- Revoir la rédaction des contrats avec les sous-traitants.

Laurent VERDES
Avocat au Barreau de Paris

Cabinet d'Avocats 23Bosquet
23 avenue Bosquet
75007 PARIS

lverdes@23bosquet.com
+33(0)1 40 62 63 26

Pierre-Yves COUTURIER
Avocat au Barreau de Paris

Cabinet d'Avocats 23Bosquet
23 avenue Bosquet
75007 PARIS

pycouturier@23bosquet.com
+33(0)1 40 62 63 20