Règlement européen sur la protection des données personnelles (RGPD)

Ce qu'il faut savoir d'ici 2018

MEDEF

A l'ère du numérique, les données constituent un enjeu majeur pour les entreprises, notamment pour celles dont l'activité s'exerce dans un cadre mondialisé. Dans ce contexte, les institutions européennes ont estimé qu'il était primordial de rappeler que la **protection des données personnelles est un droit fondamental pour les individus** et qu'à ce titre, ces données ne peuvent faire l'objet d'un quelconque droit de propriété, tant des entreprises que des personnes concernées, qui **ne peuvent disposer que d'un droit de contrôle sur ces données.** A cette fin, les institutions européennes ont décidé de mettre en place un cadre de protection des données solide et cohérent dans l'Union européenne.

Les données personnelles ne peuvent pas faire l'objet d'un droit de propriété : ni les personnes, ni les entreprises ne peuvent être propriétaires de données personnelles.

Le 27 avril 2016, le Parlement européen et le Conseil de l'Union européenne ont donc adopté le Règlement général pour la protection des données personnelles (RGPD).

Ce règlement a vocation à remplacer la directive européenne 95/46/CE du 24 octobre 1995 et à harmoniser le droit européen en matière de données personnelles qui, jusqu'à présent, laissait subsister des spécificités et de fortes disparités dans les Etats membres.

Le RGPD ne sera applicable en France qu'à partir du 25 mai 2018. La loi Informatique et Libertés du 6 janvier 1978 reste donc applicable jusqu'en 2018.

S'agissant d'un règlement, le **RGPD sera directement applicable en France à partir du 25 mai 2018** et il prévaudra sur les législations nationales. La loi du 6 janvier 1978 modifiée, dite « Loi Informatique et Libertés », reste donc applicable jusqu'à cette date, la France ayant jusqu'au 25 mai 2018 pour se mettre en conformité avec le Règlement et pour réviser la loi française.

Si le règlement reprend largement les principes contenus dans la directive de 1995, il responsabilise également les entités qui collectent ou traitent des données personnelles, les obligeant notamment à vérifier la conformité de leurs traitements et à notifier les failles de sécurité les plus graves, ainsi qu'en les soumettant à des sanctions administratives dont les plafonds ont été considérablement relevés.

Il est donc indispensable pour les entreprises françaises de commencer à se préparer à la mise en œuvre du règlement européen pour être prêtes en mai 2018.

1. Les questions à se poser

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

Donnée à caractère personnel : toute information se rapportant à une **personne physique** identifiée ou identifiable (par un nom, un numéro, une donnée de localisation, une donnée de connexion…).

Données sensibles (au sens de la protection des données) : données susceptibles de donner lieu à discrimination (origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, orientation sexuelle…) ou propres à une personne (données génétiques, biométriques, de santé).

Traitement : toute opération (automatisée ou non) sur des données à caractère personnel (collecte, enregistrement, organisation, stockage, conservation, adaptation, modification, extraction, utilisation, communication par transmission, rapprochement ou interconnexion…).

Responsable du traitement (« *data controller* ») : personne, service ou organisme (public ou privé : entreprises, administrations, associations…) qui détermine les finalités et les moyens du traitement (= **donneur d'ordres**).

Sous-traitant (« *data processor* ») : personne, service ou organisme (public ou privé) qui traite des données personnelles pour le compte du responsable de traitement.

♦ Quand doit-on appliquer le RGPD ?

Le règlement européen s'applique aux traitements de données personnelles lorsque :

- le **traitement a lieu sur le territoire de l'Union européenne**, ou
- le **responsable de traitement ou le sous-traitant sont établis sur le territoire de l'Union** européenne (même si le traitement est effectué hors de l'Union européenne), ou
- les **personnes concernées par le traitement sont des citoyens ou ressortissants européens.**

2. Le renforcement des obligations du responsable de traitement

Le règlement européen a pour objectif de renforcer la responsabilité des entités qui mettent en place des traitements de données personnelles, en les incitant à **jouer un rôle actif dans le contrôle de la conformité de leurs traitements au règlement**. **C'est le système de *l'accountability***. Ce renforcement des obligations du responsable de traitement se traduit notamment par :

♦ La suppression des formalités préalables

Le règlement européen **ne prévoit plus de mesures de déclarations préalables des traitements**, mais il responsabilise le responsable du traitement qui doit être **en mesure de démontrer qu'il a mis en place toutes les mesures techniques et organisationnelles appropriées** pour être en conformité avec les dispositions législatives.

Aucune déclaration à la CNIL n'est nécessaire pour la mise en œuvre d'un traitement.

Pour ce faire, il doit mettre en place :

- une **politique interne** en matière de protection des données personnelles ;
- des **mesures de traçabilité** pour prouver la conformité des traitements (obligation de documenter) ;
- des **mesures appropriées « *by design* » et « *by default* »**, c'est-à-dire que le responsable de traitement doit s'assurer, dès la conception de l'architecture du traitement, qu'il existe des paramètres par défaut protecteurs (tels que l'anonymisation, la restriction des accès, la traçabilité…).

♦ *L'accountability* et le renforcement de la sécurité

En contrepartie de l'assouplissement des formalités, le responsable du traitement doit mettre en place des procédures internes afin de veiller au respect du règlement et de prouver cette conformité. Pour ce faire, il doit notamment **mettre en place toutes les mesures techniques et organisationnelles pour assurer un niveau de sécurité approprié aux risques** (pseudonymisation, cryptage des données, traçabilité…).

➢ **L'obligation d'effectuer des analyses d'impact**

Le responsable du traitement doit réaliser une étude d'impact sur chaque traitement de données personnelles. En cas de risque grave, il doit consulter la CNIL.

Alors que la loi de 1978 impose systématiquement au responsable de traitement de demander l'autorisation à la CNIL pour mettre en place les traitements les plus sensibles, le règlement ne prévoit plus cette demande d'autorisation préalable. Toutefois, le responsable de traitement doit procéder lui-même à une évaluation de son projet préalablement à la mise en place du traitement.

Ainsi, notamment lorsqu'un traitement de données personnelles utilise de nouvelles technologies et qu'il en résulte un grave risque pour les données et les individus, **le responsable de traitement doit, avec l'aide du *Data Protection Officer* (DPO), réaliser une analyse d'impact avant la mise en place du traitement**.

La CNIL devrait publier une liste de traitements ne nécessitant pas d'étude d'impact.

Lorsque l'analyse d'impact révèle un grave risque d'atteinte aux données personnelles, le responsable du traitement devra obligatoirement consulter la CNIL préalablement à la mise en place du traitement.

➢ **L'obligation de notifier les violations de données personnelles**

- ***Obligation de notifier à la CNIL***

Jusqu'à présent, seuls les opérateurs de communication électronique avaient une obligation de notifier les violations de données à caractère personnel à la CNIL et aux personnes concernées. Le règlement européen généralise cette obligation à tout responsable de traitement.

En cas de violation de données personnelles, le responsable du traitement doit le notifier à la CNIL dans les 72h de la découverte de cette violation.

En effet, **le responsable du traitement devra désormais avertir la CNIL de toute violation de données personnelles** (c'est-à-dire **toute faille de sécurité ayant entraîné la destruction, la perte, l'altération, la révélation ou l'accès non autorisé à ces données de manière intentionnelle ou accidentelle**), sauf s'il est peu probable qu'il en résulte un risque pour les personnes.

Cette notification devra intervenir sans retard injustifié, **si possible dans les 72h à compter de la connaissance de cette violation de données**.

- ***Obligation d'avertir les personnes concernées***

Par ailleurs, **le responsable de traitement devra également avertir les personnes concernées de la violation de leurs données personnelles lorsqu'il y a un grave risque d'atteinte à leurs droits et libertés**. Cette information doit intervenir sans retard injustifié.

Le responsable de traitement pourra cependant **s'exonérer de cette obligation** d'avertir les personnes concernées s'il démontre qu'il a mis en place les mesures de protection appropriées pour les données concernées (notamment l'anonymisation), s'il a pris des mesures suffisantes pour empêcher tout risque d'atteinte ou encore si l'information aux personnes concernées nécessite un effort disproportionné (dans ce cas, la notification individuelle pourrait être remplacée par une mesure publique).

Il est donc essentiel de mettre en place toutes les mesures de sécurité adaptées et d'en conserver une trace écrite.

♦ La désignation (obligatoire) d'un DPO

Les responsables de traitements et les sous-traitants **dont la principale activité nécessite le traitement régulier de nombreuses données à caractère personnel** (hors données RH de leurs salariés) doivent obligatoirement désigner un *Data Protection Officer* (DPO), **peu importe la taille de l'entreprise**.

Un DPO doit être désigné lorsque l'entreprise traite régulièrement de nombreuses données personnelles.

Plusieurs entreprises pourront éventuellement désigner un DPO unique, facilement accessible.

Le DPO doit être désigné sur la base de ses qualités professionnelles et sur sa connaissance du droit et des pratiques en matière de données personnelles. **Il peut être salarié ou extérieur à l'entreprise** (avocat, consultant…). Toutefois, le DPO doit exercer ses fonctions **en toute indépendance** vis-à-vis du responsable du traitement, y compris lorsqu'il s'agit d'un salarié.

Le DPO a pour tâches :

- d'informer et de conseiller le responsable du traitement ou le sous-traitant et les salariés de leurs obligations découlant de la législation en matière de données personnelles ;
- de veiller à la conformité de ces législations ;
- de coopérer et d'être l'interlocuteur privilégié de la CNIL ;
- d'être le point de contact des personnes concernées par un traitement de données personnelles pour toutes les questions relatives à ce traitement et pour l'exercice des droits que leur confère le règlement.

♦ La responsabilisation des sous-traitants et la coresponsabilité

➢ Comment désigner le responsable du traitement ?

Le règlement reconnaît qu'il puisse y avoir **plusieurs responsables pour un même traitement** lorsqu'ils ont déterminé ensemble les finalités et les moyens du traitement de données à caractère personnel. Les coresponsables doivent alors préciser leurs rôles respectifs à l'égard des personnes concernées par le traitement. Ces dernières pourront indifféremment exercer leurs droits auprès de chacun des coresponsables et, en cas de sanctions, tous les coresponsables devront payer l'amende.

➢ Comment choisir son sous-traitant ?

Le règlement impose au responsable du traitement de **choisir un sous-traitant qui assure des garanties de protection suffisantes** dans le traitement des données personnelles. Le **contrat de sous-traitance est obligatoire** et il doit contenir des stipulations pour imposer au sous-traitant de :

- traiter les données personnelles selon les seules instructions du responsable du traitement ;
- s'assurer de la confidentialité du traitement des données ;
- prendre les mesures de sécurité appropriées et assurer le respect de ces mesures ;
- respecter les conditions prévues en cas de sous-traitance ultérieure ;
- supprimer ou rendre au responsable du traitement toutes les données personnelles à la fin de la mission de traitement qui lui a été confiée ;
- tenir à disposition du responsable du traitement toutes les informations nécessaires à démontrer la conformité au règlement et lui permettre d'auditer ou de contrôler ;
- avertir le responsable du traitement le plus tôt possible de toute violation de données.

Le sous-traitant doit rendre des comptes au responsable du traitement et respecter ses consignes. Dans le cas contraire, il peut être soumis aux mêmes sanctions qu'un coresponsable de traitement.

Le sous-traitant ne peut pas lui-même sous-traiter sans le consentement préalable écrit du responsable de traitement.

Le sous-traitant qui **outrepasse les missions qui lui sont confiées** doit être **considéré comme responsable de traitement** dans la mesure où il détermine, sans autorisation, les finalités et les moyens du traitement. Il est alors soumis aux mêmes obligations en tant que coresponsable du traitement.

♦ L'encadrement des transferts hors UE

Tout transfert de données à caractère personnel vers un organisme situé dans un pays n'appartenant pas à l'Union européenne est en principe interdit sauf si l'une des conditions suivantes est remplie :

La Commission européenne estime que cet Etat assure un niveau de protection adéquat.

La Commission européenne peut constater par voie de décision qu'un pays tiers à l'Union européenne assure un niveau de protection adéquat. C'est par exemple le cas d'Israël, du Canada, de la Suisse ou encore de l'Argentine[1].
Liste des pays reconnus adéquats par l'Union européenne

Le transfert entre dans le cadre du Privacy Shield.

Le *Privacy Shield* est un accord entre l'UE et les Etats-Unis permettant le transfert de données personnelles **vers les entreprises adhérentes qui sont situées sur le sol américain** et qui doivent respecter les conditions de protection des données personnelles. Avant tout transfert vers les Etats-Unis, il faut donc **s'assurer que l'entreprise est adhérente au *Privacy Shield***.

Le responsable de traitement a prévu des garanties appropriées et suffisantes.

Le responsable de traitement peut transférer des données personnelles vers une entreprise située dans un Etat ne faisant pas l'objet d'une décision de la Commission européenne s'il existe des garanties appropriées[2,3,4], telles que :

- *Clauses contractuelles types*
- *Binding Corporate Rules (BCR)*
- *Autorisation de la CNIL*

Le transfert entre dans l'une des exceptions prévues par le RGPD.

Le règlement européen prévoit que les données personnelles peuvent être **exceptionnellement** transférées vers un Etat hors UE. Ce transfert ne doit **pas** revêtir **de caractère répétitif**, il doit concerner un **nombre limité de personnes** et il doit offrir des **garanties appropriées**. Ces exceptions sont :

- *Le consentement des personnes*
- *L'exécution légitime d'un contrat*
- *L'exercice d'un droit de consultation*
- *Le respect d'une décision de justice*

♦ L'alourdissement des sanctions

➢ Sanctions administratives

Les institutions européennes ont voulu responsabiliser les acteurs à l'égard des traitements de données personnelles en fixant un **plafond de sanctions administratives élevé**. Ainsi, alors que la loi de 1978 plafonnait les sanctions à un montant de 150 000 €, le règlement européen prévoit que **la CNIL peut prononcer des amendes** dont le montant peut atteindre jusqu'à :

- **2 % du chiffre d'affaires annuel mondial** de l'entreprise concernée (ou 10 000 000 € pour les autres entités) ;
- **4 % du chiffre d'affaires annuel mondial** de l'entreprise concernée (ou 20 000 000 € pour les autres entités) pour les atteintes les plus graves (non-respect du consentement ou des droits des personnes, transfert illicite de données…).

La CNIL peut prononcer des amendes correspondant à 4 % du chiffre d'affaires annuel mondial d'une entreprise (ou 20 000 000 €).

➢ Sanctions civiles

Le responsable du traitement ou le sous-traitant devra également **indemniser toute personne ayant subi un dommage** du fait de la violation du règlement sur la protection des données personnelles.

[1] Cf. https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde
[2] Cf. https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne
[3] Cf. https://www.cnil.fr/fr/les-bcr-regles-internes-dentreprise
[4] Cf. https://www.declaration.cnil.fr/declarations/declaration/accueil.action

Une action de groupe est désormais possible afin que les personnes concernées puissent donner mandat à une association / organisation pour agir en justice à leur place et demander la cessation du dommage.

➢ **Sanctions pénales**

Enfin, en plus des sanctions civiles et administratives, les **articles 226-16 et suivants du Code pénal** incriminent les atteintes aux droits de la personne résultant de traitements informatiques. Les sanctions encourues peuvent aller jusqu'à **5 ans d'emprisonnement et 300 000 € d'amende** pour les personnes physiques et **1 500 000 € pour les personnes morales (**entreprises, associations…).

3. La mise en œuvre du traitement de données personnelles

♦ Comment mettre en place un traitement ?

Pour qu'un traitement de données personnelles soit conforme, il faut :

➢ **Vérifier que le traitement est licite**

Le traitement ne peut être créé et mis en œuvre que dans l'une des conditions suivantes :

- la personne concernée a accepté le traitement (**consentement**), ou
- le traitement est **nécessaire à l'exécution d'un contrat** dont la personne concernée est partie (il ne doit pas y avoir d'alternative possible) **ou au respect d'une obligation légale, ou**
- le traitement est nécessaire à **l'intérêt légitime du responsable du traitement**, sauf si les intérêts ou les droits des personnes concernées doivent prévaloir.

➢ **Vérifier que le traitement est loyal**

Le responsable du traitement doit vérifier que le traitement est légitime et que les données collectées sont strictement nécessaires au traitement.

Seules les données adéquates, pertinentes et nécessaires doivent être collectées. Par exemple, si une entreprise organise un jeu-concours, elle ne peut collecter que les données nécessaires pour identifier et contacter le gagnant (nom, prénom, adresse mail ou numéro de téléphone). En revanche, elle ne pourra pas collecter le numéro de sécurité sociale ou encore la plaque d'immatriculation du véhicule.

Par ailleurs, **les données doivent être collectées pour des finalités déterminées, explicites et légitimes**. Par exemple, dans le cadre d'un jeu-concours, la collecte des données est nécessaire à l'organisation du jeu afin d'identifier le gagnant et de lui remettre le lot.

➢ **Obtenir le consentement de la personne concernée** (si les autres conditions ne s'appliquent pas)

Le règlement précise que le consentement doit consister en « ***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* », l'accord pouvant indifféremment être donné **par écrit, y compris sous forme électronique, par oral** ou par tout autre acte positif. **Le consentement peut être retiré à tout moment par la personne concernée.**

En matière de prospection électronique (emailing), le consentement reste le principe.

A titre d'exemple, le fait de cocher des cases ou encore de paramétrer les options d'un site peut constituer un acte positif clair au sens du RGPD[5].

En revanche, **le silence, l'inactivité et l'inaction** (comme les cases pré-cochées par exemple) **ne peuvent pas valoir consentement**.

Pour les traitements comportant des **données sensibles** (au sens de la protection des données personnelles), la personne concernée doit avoir donné **son consentement explicite** (ce qui semble supposer obligatoirement un écrit).

[5] Cf. Recommandation de la CNIL n° 2013-378 du 5 décembre 2013 relative aux cookies et autres traceurs.

Le responsable du traitement doit s'assurer que la personne concernée par un traitement a donné son consentement à l'utilisation ou la collecte de ses données. Ce consentement doit être nécessairement par écrit en cas de traitement de données dites sensibles.

Il **appartient au responsable de traitement de prouver que chaque personne a consenti** de manière libre, éclairée et non-équivoque au traitement de ses données personnelles (**ce qui suppose qu'elle soit informée préalablement**), notamment en conservant une trace de ce consentement.

♦ Comment informer les personnes de l'existence d'un traitement (obligatoire) ?

Le responsable du traitement a l'obligation d'informer les personnes concernées de l'existence d'un traitement de données personnelles au moment de la collecte de leurs données. **Cette information doit être donnée par écrit** (mentions sur un contrat ou formulaire spécifique, CGV, mentions légales sur un site internet, règlement, facture…), sauf demande expresse de la personne concernée.

Pour répondre à cette exigence, le responsable du traitement doit indiquer :

- l'identité et les coordonnées du responsable de traitement et les coordonnées du *Data Protection Officer* (DPO) s'il a été désigné ;
- les finalités du traitement et la base juridique du traitement (consentement, exécution d'un contrat, exécution d'une obligation légale…) ;
- les destinataires ou catégories de destinataires des données (par exemple : les conseillers clientèle, les responsables RH…) ;
- les éventuels transferts de données hors Union européenne ;
- la durée de conservation des données ou les critères utilisés pour déterminer cette durée ;
- les droits des personnes concernées (accès, rectification, suppression, opposition…) ;
- le droit d'introduire une réclamation auprès de la CNIL.

Par ailleurs, **le responsable du traitement et le sous-traitant** ont l'obligation (**pour les entreprises de plus de 250 salariés**) de tenir à jour un registre de leurs traitements (qui peut prendre la forme d'un tableau Excel) sur lequel doivent figurer certaines informations (pour chacun des traitements) :

- l'identité et les coordonnées du responsable du traitement (ou du sous-traitant), ainsi que les coordonnées du DPO s'il a été désigné,
- les finalités du traitement,
- les catégories des données collectées,
- les destinataires des données collectées,
- les éventuels transferts de données à un pays situé hors UE,
- les durées de conservation des données,
- les mesures de sécurité mises en place.

4. L'exécution du traitement de données personnelles

♦ Comment utiliser les données ?

Les données collectées ne doivent normalement être utilisées que pour les finalités prévues initialement. Cependant, ces données peuvent être réutilisées à d'autres fins dans l'un des cas suivants :

- la personne concernée a donné son **consentement**,
- les nouvelles finalités envisagées sont **compatibles** avec les finalités initialement prévues (au regard du contexte, de la relation qui existe entre le responsable du traitement et la personne concernée ou encore des mesures de sécurité mises en place par exemple).

♦ Quels sont les droits des personnes concernées par un traitement ?

Le responsable du traitement doit **informer par écrit** les personnes concernées par un traitement de l'existence et des modalités d'exercice de leurs droits au regard des traitements de données personnelles.

En effet, toute personne concernée par un tel traitement dispose de droits :

- **Un droit d'accès** : **obtenir la confirmation du traitement** de ses données et des modalités de ce traitement (finalités, destinataires, durée de conservation…) et **recevoir copie de toutes les informations la concernant** ;
- **Un droit de rectification** : demander la rectification de ses données personnelles ;
- **Un droit à la portabilité** : récupérer les données personnelles la concernant qu'elle avait elle-même fournies au responsable de traitement, dans un format ouvert et lisible ou transmettre directement ces données à un autre responsable de traitement.
- **Un droit d'opposition** : s'opposer au traitement à tout moment, y compris pour la prospection commerciale ;
- **Un droit de suppression** (droit à l'oubli) : obtenir la suppression de ses données personnelles si :
  - elles ne sont plus nécessaires au regard de la finalité pour lesquelles elles ont été collectées,
  - la personne a retiré son consentement à un traitement basé sur celui-ci,
  - la personne s'oppose au traitement,
  - les données sont traitées de manière illicite ou illégale.

NB : **Le règlement ne s'applique pas aux données des personnes décédées**, mais, en France, **la loi pour une République numérique** prévoit qu'une personne **peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données personnelles après son décès**.

Le responsable de traitement doit **mettre à disposition** des personnes concernées un **moyen d'exercer gratuitement leurs droits** et il doit **répondre** dans un délai **d'un mois maximum** à toute demande d'une personne concernée par un traitement. **Il ne peut refuser de faire droit à cette demande**, sauf si elle est manifestement excessive.

5. La fin du traitement de données personnelles

Les données personnelles ne doivent être conservées que pour la durée strictement nécessaire au but poursuivi par le responsable du traitement. **A l'issue du traitement ou de la durée prévue, les données doivent être détruites ou restituées aux personnes concernées, sans qu'aucune copie ne soit conservée**.

Cependant, ces données **peuvent être conservées au-delà si elles sont anonymisées**, c'est-à-dire s'il est impossible par un quelconque moyen d'associer ces données à une personne.

Les données personnelles doivent être détruites à l'issue du traitement, sauf si elles ont été totalement anonymisées.

Le règlement précise que la « **pseudonymisation** » des données (c'est-à-dire le mécanisme d'anonymisation réversible) **n'est pas une mesure suffisante** pour permettre leur conservation au-delà de la durée nécessaire au traitement. En effet, même si elle réduit les risques d'atteinte aux données personnelles, elle ne permet pas d'anonymiser définitivement ces données, qui peuvent continuer à être associées à une personne en effectuant certains recoupements.