Entré en vigueur le 25 mai 2018 dans toute l'Union européenne, le Règlement général sur la protection des données (RGPD) instaure un nouveau cadre juridique pour la protection des données personnelles.

Toute entreprise qui réalise un traitement de données (gestion de la paie, recrutement, fichier clients ou fournisseurs...) doit respecter le **Règlement général sur la protection des données (RGPD)**. Il s'applique à **toute entreprise**, **quelle que soit sa taille et son secteur d'activité**, dès lors qu'elle est établie sur le territoire de l'Union européenne ou que son activité cible directement des résidents européens.

Une donnée personnelle ou « *donnée à caractère personnel* » est une **information se rapportant à une personne physique identifiée ou identifiable** (ex : nom, prénom, numéro de sécurité sociale, adresse, numéro de téléphone, adresse électronique, photo, empreinte, donnée de géolocalisation, adresse IP ou identifiant en ligne).

Une personne est dite **identifiée** lorsque l'on connaît son identité. Une personne est **identifiable** lorsqu'elle peut être identifiée, quand bien même ses nom et prénom resteraient inconnus, à partir du **croisement d'un ensemble de données** (ex : une femme vivant à telle adresse, née tel jour et membre de telle association).

Un traitement de données personnelles consiste en **toute opération portant sur des données personnelles**, quel que soit le procédé utilisé (ex : la collecte, l'enregistrement, la conservation, la modification, la consultation, la diffusion ou l'effacement de données).

Autrement dit, on parle de traitement de données dès que les données d'une personne sont utilisées d'une manière ou d'une autre et peu importe à qui appartiennent ces données (un **client**, un **fournisseur**, un **prestataire**, un **employé**, un **candidat à l'embauche**, etc.).

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

Pour être conforme au RGPD, le traitement de données doit obéir aux **principes suivants** :

- Le traitement doit être **licite** : il doit être fondé sur l'une des 6 bases légales fixées par le RGPD notamment le consentement de la personne concernée, l'exécution d'un contrat ou le respect d'une obligation légale.
- Le traitement doit être **transparent** : la personne dont les données sont collectées doit être informée de la collecte et de sa finalité, ainsi que des droits dont elle dispose sur ses données (accès, rectification, portabilité, effacement...).

- Le traitement doit avoir une **finalité** : le responsable du traitement doit définir l'objectif poursuivi par la collecte des données. Les données ne doivent pas être traitées d'une manière incompatible avec cette finalité.
- Le traitement doit être **proportionnel et pertinent** : seules les données strictement nécessaires à la réalisation de l'objectif peuvent être collectées. On parle de « *principe de minimisation* ».
- Le traitement doit être **temporaire** : la durée de conservation des informations doit être définie dès la mise en place du dispositif qui collecte ces données. Une fois l'objectif atteint, les informations collectées ne sont plus nécessaires et doivent donc être supprimées.
- Le traitement doit être **sécurisé** : toutes les mesures nécessaires pour garantir la sécurité, et notamment la confidentialité des données personnelles doivent être mises en place (ex : mots de passe, https, sauvegarde). Ces mesures de sécurité sont proportionnelles aux risques encourus (ex : vol ou perte de données).

Le représentant légal est désigné « **responsable du traitement** ». Le responsable du traitement est la personne **à l'initiative du traitement de données**, il détermine ses finalités et ses moyens.

Le plus souvent, le responsable de traitement a recours à un **sous-traitant** chargé de traiter les données pour le compte du responsable du traitement (ex : Hello asso, …).

Le responsable du traitement et son sous-traitant doivent respecter de **nombreuses obligations** en matière de protection des données personnelles.

Quelles informations faut-il délivrer ?

Le responsable du traitement doit transmettre les **informations suivantes** :

- Identité et coordonnées du responsable du traitement
- Finalité poursuivie par le traitement : c'est-à-dire à quoi vont servir les données personnelles collectées
- Base légale justifiant le traitement : il peut s'agir du consentement de la personne, du respect d'une obligation prévue par un texte de loi, de l'exécution d'un contrat, etc.
- Caractère obligatoire ou facultatif de la fourniture de données personnelles : les conséquences pour la personne en cas de non-fourniture des données
- Destinataires des données personnelles : qui va recevoir et accéder aux données (service interne compétent, prestataire, etc.)
- Durée de conservation des données personnelles

- Droits de la personne sur ses données : droit de refuser la collecte, droit d'accéder, de rectifier et d'effacer ses données
- Droit de la personne d'introduire une réclamation auprès de la Cnil
- Source d'où proviennent les données personnelles, en cas de collecte indirecte

Les informations doivent être transmises de façon **concise, transparente, compréhensible et facilement accessible**, en des termes clairs et simples.

Quelle sanction en l'absence d'information ?

Le fait de ne pas informer la personne auprès de laquelle sont recueillies des données est puni d'une **amende pénale** de **1 500 €** pour les entrepreneurs individuels et **7 500 €** pour les sociétés.

Le recueil de consentement est-il toujours obligatoire ?

Le recueil du consentement est **obligatoire**, à moins que le traitement soit justifié par **l'exécution d'un contrat** (ex : contrat de travail, contrat de vente, de location).

De plus, le recueil de consentement est **toujours obligatoire** dans les cas suivants :

- Collecte de **données personnelles « sensibles »**. Il s'agit d'une catégorie de données éminemment personnelles qui sont susceptibles de conduire à des discriminations si elles sont révélées (ex : origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, orientation sexuelle, appartenance syndicale, données génétiques).

Comment recueillir un consentement valable ?

Pour être valable, le consentement obtenu doit remplir les **4 conditions suivantes** :

- Le consentement doit être **libre** : il ne doit être ni contraint ni influencé.
- Le consentement doit être **éclairé** : avant de consentir, la personne concernée doit avoir reçu une information suffisante de manière à pouvoir décider en toute connaissance de cause. L'information doit être communiquée en des termes clairs et facilement compréhensibles.
- Le consentement doit être **spécifique** : si le traitement comporte plusieurs finalités (ex : gestion de clientèle, enquête de satisfaction, opération de prospection).
- Le consentement doit être **univoque** : il doit être donné par un acte délibéré, sans aucune ambiguïté. Il peut être recueilli, par exemple, au moyen d'une déclaration écrite ou orale ou via le cochage d'une case par voie électronique.

Quelle sanction en l'absence de consentement ?

Lorsque le recueil de consentement est obligatoire, le traitement de données personnelles obtenues **sans le consentement** de la personne concernée est puni pénalement de **5 ans** d'emprisonnement.

Droit à l'effacement des données (« droit à l'oubli »)

Le responsable du traitement doit permettre, à la personne qui en fait la demande, d'obtenir **l'effacement de ses données** dans les meilleurs délais.

Ce « droit à l'oubli » n'est pas général, il s'applique **uniquement dans les cas suivants** :

- Les données personnelles ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière.
- La personne concernée s'oppose au traitement et il n'existe pas de motif légitime pour le traitement.
- Les données personnelles ont fait l'objet d'un traitement illicite (ex : le consentement de la personne n'a pas été recueilli alors qu'il était obligatoire)
- Les données personnelles doivent être effacées pour respecter une obligation légale prévue par le droit de l'UE ou par le droit de l'État membre auquel le responsable du traitement est soumis.

Recenser les traitements de données

Le responsable du traitement doit **recenser les traitements** de données personnelles (automatisés ou non) **et les supports** sur lesquels ces traitements reposent, c'est-à-dire :

- Les matériels (ex. : serveurs, ordinateurs portables, disques durs)
- Les logiciels (ex. : systèmes d'exploitation, logiciels métier)
- Les canaux de communication logiques ou physiques (ex. : fibre optique, Wi-Fi, Internet, échanges verbaux, coursiers)
- Les supports papier (ex. : documents imprimés, photocopies)
- Les locaux et installations physiques où se situent les éléments précédemment cités (ex. : locaux informatiques, bureaux).

Apprécier les risques liés à chaque traitement

Ce recensement permet d'**apprécier les risques** engendrés par chaque traitement, notamment :

- **Accès illégitime à des données** (ex : usurpation d'identité consécutive à la divulgation de renseignements figurant sur des documents personnels)

Le responsable du traitement doit identifier les **sources de risques** en prenant en compte des sources humaines (ex : administrateur informatique, utilisateur, attaquant externe, concurrent).

Sensibiliser les utilisateurs

De plus, il doit **rédiger une charte informatique**, annexée au règlement intérieur, comportant les informations suivantes :

- Règles de protection des données et sanctions encourues en cas de manquement
- Champ d'application de la charte (ex : modalités d'intervention des équipes chargées de la gestion des données, moyens d'authentification, règles de sécurité)
- Modalités d'utilisation des moyens informatiques mis à disposition (poste de travail, espace de stockage, accès à internet, messagerie électronique...)
- Conditions d'administration du système d'information
- Responsabilités et sanctions encourues en cas de non-respect de la charte.

Sauvegarder et archiver les données

Le responsable du traitement doit **effectuer des sauvegardes régulières** pour limiter l'impact d'une disparition ou d'une altération non désirée de données. Il est également recommandé de stocker au moins une **sauvegarde sur un site extérieur** et d'isoler une **sauvegarde hors ligne**, déconnectée du réseau de l'entreprise.

Par ailleurs, le responsable doit **archiver les données qui ne sont plus utilisées au quotidien** mais qui n'ont pas encore atteint leur durée limite de conservation, par exemple parce qu'elles sont conservées afin d'être utilisées en cas de litige.

Pour ce faire, il doit définir un processus de gestion des archives qui appellent plusieurs questions, notamment :

- Quelles données doivent être archivées ?
- Comment et où sont-elles stockées ?
- Quelles sont les modalités d'accès spécifiques aux données archivées ? (L'utilisation d'une archive doit intervenir de manière ponctuelle et exceptionnelle)
- S'agissant de la destruction des archives, quel mode opératoire faut-il choisir pour garantir que l'intégralité d'une archive a été détruite ?