Le Règlement européen sur la protection des données personnelles (RGPD) : Comment se mettre en conformité ?

Le Règlement général sur la protection des données personnelles est applicable à partir du 25 mai 2018. Il vise à renforcer la protection des données personnelles. La mise en conformité est importante puisqu'en cas de non-respect, les professionnels encourent une sanction pouvant aller jusqu'à 4% du chiffre d'affaires.

En pratique, la plupart des formalités préalables actuelles auprès de la CNIL (déclarations, autorisations) vont disparaître. Vous devez désormais mettre en place un dispositif interne de gestion et de protection des données personnelles que vous traitez et produire les preuves que vous vous êtes mis en conformité.

Afin de répondre à vos principales interrogations et vous guider dans cette démarche, vous trouverez ci-après nos préconisations.

ETAPE 1 : Savoir si je suis concerné

- ✓ **Quelles sont les entreprises visées ?**

L'ensemble des entreprises, quel que soit leur effectif, dès lors qu'elles traitent des données personnelles de personnes se trouvant sur le territoire de l'union européenne.

- ✓ **Quels sont les types de données considérées comme personnelles ?**

Toute information permettant d'identifier une personne physique (salarié, fournisseur, client, sous-traitant, etc) directement ou indirectement.

Exemples : nom, adresse électronique, adresse IP, numéro de sécurité sociale, identifiant professionnel, image, données de localisation, etc.

- ✓ **Qu'est-ce qu'un traitement ?**

Toute opération (automatisée ou non) portant sur des données personnelles : collecte, conservation, stockage, utilisation….

Exemples : gestion de la clientèle (fichiers de prospection), gestion RH (recrutement, paies, discipline, formation), newsletters, vidéosurveillance, contrôles d'accès, biométrie, géolocalisation, etc.

Un traitement de données doit avoir un objectif, une finalité. À chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de votre activité professionnelle.

- ✓ **Qui gère les données personnelles ?**

Il y a deux intervenants :

1. Le responsable de traitement = la personne, le service, la direction ou l'entreprise qui décide de mettre en place un traitement et en définit les finalités et moyens → Le chef d'entreprise dans les PME, le DSI, le directeur d'activité, etc...

2. Le sous-traitant = la personne, le service, la direction ou l'entreprise qui traite des données personnelles pour le compte du responsable du traitement.

Exemples : prestataires de paie externes, prestataires informatiques, prestataires chargés de la prospection commerciale …

➔ Si je réponds à ces conditions alors je dois respecter le nouveau texte et adapter mes process.

ETAPE 2 : Je suis concerné par le RGPD, que dois-je faire en amont ?

Les formalités ci-dessous sont une préconisation afin de faciliter votre mise en conformité avec les différentes obligations du règlement et vous permettront de prouver facilement votre démarche en cas de contrôle. Elles ont été choisies conformément aux recommandations de la CNIL.

https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf

Désigner un pilote

Le pilote (ou DPO) a pour rôle de contrôler la conformité des traitements et de conseiller l'entreprise. Il peut être un salarié de l'entreprise ayant des compétences en la matière ou une personne extérieure présentant dans les deux cas des garanties d'indépendance (pour les PME, il est conseillé d'appliquer cette dernière option). Il s'agit donc d'une personne distincte du responsable de traitement.

BON A SAVOIR : Le DPO est obligatoire :
-si votre activité principale vous amène à réaliser un suivi régulier et systématique des personnes à grande échelle ;
-si vous traitez des données sensibles à grande échelle. Les CNIL européennes (G29) ont récemment diffusé quelques critères pour préciser cette notion : nombre de personnes concernées, volume de données traitées, durée ou permanence des activités de traitement, étendue géographique de l'activité de traitement.
Nous vous conseillons toutefois de nommer un DPO.

➔ La CNIL a mis en ligne un formulaire de désignation du DPO ici.

Cartographier vos traitements de données personnelles

Commencez par recenser de façon précise les traitements de données personnelles que vous mettez en œuvre. Ce recensement peut se faire via l'établissement d'un registre qui doit répondre aux questions suivantes :

1. QUI TRAITE LES DONNÉES ? (responsable du traitement, DPO, responsable des services opérationnels , sous-traitant)
2. QUELLES DONNÉES ?
3. POURQUOI ? = les finalités pour lesquelles vous collectez ou traitez ces données (gestion de la relation commerciale, gestion RH, etc.)
4. OÙ SONT-ELLES HERBERGÉES ?
5. JUSQU'À QUAND ?
6. COMMENT SONT-ELLES PROTEGÉES ?

La CNIL propose un modèle de registre. Pour les consulter, **reportez-vous à l'annexe.**

BON A SAVOIR : Le registre des traitements n'est pas obligatoire pour les entreprises comptant moins de 250 salariés, sauf, notamment :
-si le traitement n'est pas occasionnel ;
-si le traitement porte sur des données « sensibles » (les données concernant l'origine raciale ou ethnique, la religion, les opinions politiques, l'appartenance à un syndicat, la santé, la vie sexuelle ou l'orientation sexuelle d'une personne, données biométriques, etc).

Dans la mesure où, en matière sociale, le traitement des données relatives à la paie est permanent, la tenue de ce registre est donc essentielle. Le registre est placé sous la responsabilité du dirigeant de l'entreprise.

Prioriser les actions

Vous devez identifier les actions à mener pour vous conformer aux obligations actuelles et à venir. Par exemple :

1. Assurez-vous que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées ;

2. Identifiez la base juridique sur laquelle se fonde votre traitement ;

Exemples : transmission de certaines données personnelles à l'administration fiscale ou à la sécurité sociale, exécution d'un contrat, prévention de la fraude, impératif de sécurité, etc.

3. Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités ;

La CNIL a mis à disposition un guide relatif aux sous-traitants **avec un modèle de clause spécifique que vous pouvez ajouter dans vos contrats. En la signant, les sous-traitants sont censés avoir pris connaissance de ces nouvelles règles.** Pour le consulter, cliquez ici

4. Vérifiez les mesures de sécurité mises en place en interne.

Gérer les risques

Si vous avez identifié des traitements à risque, vous devrez mener, pour chacun de ces traitements, une étude d'impact sur la protection des données.
Un traitement est à risque lorsqu'il est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Exemples :

- *collecte de données sensibles ;*
- *collecte de données personnelles à grande échelle ;*
- *personnes vulnérables (patients, personnes âgées, enfants, etc.) ;*
- *usage innovant ou utilisation d'une nouvelle technologie ;*
- *transferts de données hors Union Européenne*

La CNIL a développé des outils pratiques sur le sujet. Pour les consulter cliquez ici

Organiser
les processus internes

Pour garantir un haut niveau de protection des données personnelles, mettez en place des procédures internes qui garantissent la protection des données :

1. Prendre en compte la protection des données personnelles dès la conception et respecter le principe de minimisation des données (= seules les données strictement nécessaires au traitement sont collectées et traitées) ;
2. Assurer les modalités de collecte du consentement : vérifier les mentions d'informations et clauses contractuelles (ETAPE 3 page 8) ;
3. Vérifier la mise en place d'une procédure de gestion des réclamations ou demandes relatives à l'exercice des droits des personnes (ETAPE 4 page 10);
4. Garantir la sécurité des données pour éviter la destruction, la perte, l'altération ou la divulgation non autorisée des données (ETAPE 3 page 8 et ETAPE 6 page 12) ;
5. Anticiper les violations de données (ETAPE 6 page 12) ;
6. Sensibiliser les salariés et collaborateurs.

Pour cela, appuyez-vous sur les conseils du DPO.

Documenter
la conformité

Afin de prouver votre conformité, vous devez constituer un dossier documentaire permettant de démontrer que le traitement de données personnelles est conforme au règlement. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.

Exemple : votre dossier devra notamment comporter les éléments suivants :

- *Le registre des traitements ;*
- *Les mentions d'information ;*
- *Les modèles de recueil du consentement des personnes concernées ;*
- *Les procédures mises en place pour l'exercice des droits des personnes ;*
- *Les contrats avec les sous-traitants ;*
- *Les procédures internes en cas de violations de données.*

ETAPE 3 : Une fois le plan de conformité établi, comment assurer la sécurité des données personnelles ?

✓ Recueillir le consentement des personnes

1. Quand ?

Il est possible de collecter, utiliser, traiter des données personnelles sans le consentement des personnes, lorsque le traitement est nécessaire, notamment :

- À l'exécution d'un contrat

Exemples : traitement d'une adresse pour la livraison d'un produit acheté en ligne, traitement des informations figurant sur une carte de crédit afin d'effectuer une transaction

- Pour le respect d'une obligation légale

Exemples : des numéros de sécurité sociale ou des éléments de rémunération doivent être transmis à la sécurité sociale ou à l'administration fiscale

- Si l'intérêt légitime du responsable de traitement le justifie

Exemples : prévention de la fraude, sécurité du réseau informatique

a) **En matière commerciale**

Le recueil du consentement n'est obligatoire que dans certains cas notamment en cas de prospection commerciale par voie électronique et d'utilisation de cookies[1] pour certaines finalités. En cas de recueil « sur place » des données auprès d'une personne, vous devez l'informer (cf étape 5 page 11).

Pour les clients :

Le consentement n'est pas requis, à condition que votre offre commerciale concerne des produits similaires à ceux déjà fournis. Vous devez :

- Informer la personne que son adresse mail sera utilisée à des fins de prospection ;
- Lui permettre de s'opposer à cette utilisation à tout moment.

Pour les prospects :

Selon le mode de prospection (email, téléphone ou sms) que vous utilisez, les personnes sollicitées doivent au préalable avoir donné leur accord pour recevoir vos messages (pour les relations btoc) ou ne pas avoir exprimé leur refus (pour les relations btob) :

- Insérer une case à cocher par la personne pour recevoir des propositions commerciales ;
- Eviter les cases pré-cochées.

Pour les jeux-concours :

Le participant donne son consentement pour participer au jeu-concours mais pas pour être démarché par la suite. Il convient de :

- Lui donner le choix de recevoir ou non des offres de prospection commerciale (ex : case à cocher) ;
- Lui permettre de s'opposer à cette utilisation à tout moment.

Dans tous les cas, les personnes doivent pouvoir refuser de recevoir d'autres sollicitations de votre part.

[1] Un cookie est un fichier qui est déposé par votre navigateur sur votre ordinateur lorsque vous surfez sur Internet et qui trace votre activité.

b) **En matière sociale**

Le traitement des données personnelles est nécessaire à l'exécution du contrat de travail. Le consentement des salariés n'est donc pas nécessaire. Toutefois, pour les données qui ne sont pas directement liées au contrat de travail, mais qui sont nécessaires pour que le salarié puisse bénéficier d'avantages via le CE par exemple, (nombre d'enfants, âge des enfants), les données ne peuvent être collectées qu'avec le consentement du salarié.

2. Comment ?

Vous devez conserver une trace de ce consentement. L'accord des personnes doit se manifester de façon libre, spécifique, éclairée et univoque, par écrit, y compris sous forme électronique, ou par oral.

Exemples : le fait de cocher une case, le fait de paramétrer les options d'un site, le fait de remplir une déclaration indiquant clairement que la personne accepte le traitement concerné.

➔ Pour un modèle de formulaire de recueil de données, cliquez ici

✓ **Mettre en place des mesures de sécurité**

Exemples :

- *Définir un identifiant unique par utilisateur ;*
- *Imposer un renouvellement du mot de passe ;*
- *Supprimer les permissions d'accès des utilisateurs à la fin de leur contrat ;*
- *Prévoir un mécanisme de verrouillage automatique de session en cas de non-utilisation du poste pendant un temps donné ;*
- *Utiliser des antivirus régulièrement mis à jour et prévoir une politique de mise à jour régulière des logiciels.*

➔ La CNIL a mis à disposition un guide relatif aux mesures de sécurité, cliquez ici

✓ **Délais de conservation**

Les données collectées doivent être conservées un certain laps de temps, après quoi elles doivent être supprimées. Cette durée varie en fonction des types de données et selon les différents objectifs.

Exemples : Les données relatives à gestion de la paie ou le contrôle des horaires des salariés peuvent être conservées 5 ans. Les données des clients sont conservées pendant le temps de la relation commerciale. La durée de conservation des données de géolocalisation est de 2 mois et celle des données de vidéosurveillance d'1 mois. Les coordonnées d'un prospect qui ne répond à aucune sollicitation pendant 3 ans doivent être supprimées. Les données figurant dans un dossier médical doivent être conservées 10 ans.

Etape 4 : Le RGPD offre un panel de droits aux personnes dont les données sont collectées, quels sont-ils ?

- ✓ Le droit pour les personnes **d'accéder** à leurs données
- ✓ Le droit **de rectifier** les informations inexactes et de compléter les données
- ✓ Le droit **d'effacement** pour les personnes concernées

Exemples : si les données ne sont plus nécessaires, si le consentement a été retiré, si le traitement est illicite

- ✓ Le droit à la **portabilité** c'est-à-dire la possibilité pour la personne concernée d'obtenir les données collectées et de les transférer à un autre responsable de traitement sous conditions
- ✓ Le droit de **s'opposer** au traitement de ses données personnelles.

 Les personnes dont les données sont collectées doivent être informées de ces droits.

ETAPE 5 : Comment informer les personnes concernées ?

✓ **Les personnes à informer**

Vous devez informer toutes les personnes dont vous recueillez les données personnelles.

Exemple en matière sociale : ensemble des personnes travaillant dans l'établissement à quelque titre que ce soit (salariés, stagiaires…)

Exemple en matière commerciale : il s'agit des clients, des fournisseurs, des prestataires de service, etc

✓ **Les modalités de l'information**

Les informations peuvent être fournies par tous moyens (par écrit, par voie électronique…), à condition que cette information soit claire, concise, compréhensible et aisément accessible. Il peut s'agir :

- De notes d'information ;
- De courriers spécifiques ;
- D'informations figurant dans les contrats (de travail ou commerciaux).

Exemples : Si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée.

BON A SAVOIR : Voici un exemple dont vous pouvez vous inspirer[2] :

« Les données à caractère personnel ainsi collectées font l'objet d'un traitement dont le responsable est [nom de l'entreprise, direction concernée le cas échéant et adresse – à compléter selon le cas].

Ces données sont collectées [par exemple « dans le cadre de l'exécution du contrat » ou « pour des motifs de sécurité »… - à compléter selon le cas] et sont nécessaires à [par exemple « la fourniture et à l'utilisation du service » ou « à la mise en place d'un dispositif de vidéosurveillance »…- à compléter selon le cas].

Elles sont destinées aux services en charge de [à compléter selon le cas], ainsi qu'aux prestataires externes auxquels le responsable de traitement fait appel [à adapter au cas d'espèce].
Elles seront conservées pendant [indiquer une durée : par exemple « trois mois » ou « toute la durée du contrat » ou « toute la durée de l'utilisation du service »…]
Conformément à la réglementation applicable en matière de données à caractère personnel, vous disposez d'un droit d'accès, de rectification, d'opposition, de limitation du traitement, d'effacement et de portabilité de vos données que vous pouvez exercer [indiquer les modalités (par mail, par courrier…) et préciser l'adresse], en précisant vos nom, prénom, adresse et en joignant une copie recto-verso de votre pièce d'identité.
En cas de difficulté en lien avec la gestion de vos données personnelles, vous pouvez adresser une réclamation auprès du délégué à la protection des données personnelles [indiquer les coordonnées] ou auprès de la CNIL ou de toute autre autorité compétente. »

[2] Source : Medef

ETAPE 6 : Je constate qu'il y a une faille dans la sécurité des données, que dois-je faire ?

- ✓ **Définir la faille de sécurité**

Il s'agit d'un incident de sécurité.

Exemples : accès non autorisé, fuite ou perte de donnée, piratage, etc.

- ✓ **Modalités d'information (à qui, comment, dans quel délai ?)**

Lorsque la faille de sécurité est susceptible d'engendrer un risque élevé pour les droits des personnes, vous devez informer :

- Les personnes concernées par cette faille dans les meilleurs délais ;
- La CNIL dans un délai de 72 heures après avoir pris connaissance de la violation.

 La notification devrait contenir les éléments suivants :

- Une description de la nature de la violation de données, y compris, si possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif de données à caractère personnel concernées ;
- Le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel il est possible d'obtenir plus d'informations ;
- Une description des mesures prises ou envisagées, y compris des mesures visant à atténuer les éventuelles conséquences négatives ;
- Une description des conséquences probables de la violation de données.

ETAPE 7 : Relations avec la CNIL : quel est son rôle ?

✓ **Suppression de la majorité des formalités de déclaration**

Il n'y aura plus de déclaration de traitement à faire auprès de la CNIL mais il faudra que vous puissiez produire les preuves que vous vous êtes mis en conformité.

✓ **Pouvoirs de contrôle**

La CNIL continuera à procéder à des vérifications en ligne, sur audition et sur pièces.

✓ **Pouvoirs de sanction**

La CNIL peut prendre un certain nombre de mesures coercitives.

Exemple : avertissement, mise en demeure, suspension du flux des données, etc.

S'agissant des amendes administratives, elles peuvent atteindre, selon la catégorie de l'infraction, les plafonds suivants :

- 10 millions d'euros ou 2% du CA annuel mondial (montant plus élevé retenu) ;

Exemple : en cas de non tenue d'un registre des traitements

- 20 millions d'euros ou 4% du CA annuel mondial (montant plus élevé retenu).

Exemple : en cas de traitement mis en place en l'absence de consentement des personnes alors qu'il était requis

FOCUS

✓ **Les sous-traitants**

Si vous confiez le traitement de données à un sous-traitant, vous devez prévoir un contrat qui contient des mentions obligatoires. Le contrat doit notamment préciser que le sous-traitant :

- Respecte le règlement européen sur la protection des données personnelles ;
- Ne traite les données qui lui sont confiées que conformément aux instructions de l'entreprise et uniquement pour la finalité du contrat ;
- Met en place des mesures de sécurité appropriées ;
- Supprime les données personnelles à la fin de sa mission ;
- Avertit l'entreprise en cas de faille de sécurité.

L'entreprise reste responsable du traitement mais le prestataire est également soumis au règlement en tant que sous-traitant. A ce titre, il doit notamment aider les responsables de traitement.

 Le contrat permet à l'entreprise d'engager la responsabilité contractuelle de son sous-traitant en cas de manquement.

➔ La CNIL a mis à disposition un guide relatif aux sous-traitants **avec un modèle de clause spécifique**. Pour le consulter, cliquez ici

✓ **Les sous-traitants établis hors UE**

Ils restent soumis au RGPD dès lors qu'ils procèdent, pour le compte de leur client, à des traitements de données de personnes se trouvant dans l'UE.

Vous devez vérifier le pays d'établissement du partenaire ou sous-traitant et la possibilité de transférer les données vers ce pays. En effet, le transfert n'est possible qu'en cas notamment d'autorisation de la CNIL ou d'accord international (Privacy Shield pour les Etats-Unis par exemple).

 L'utilisation de cloud est considérée comme un transfert de données personnelles si les serveurs sont situés hors de l'Union européenne.

- ✓ **Les données biométriques**

Les données biométriques sont considérées comme des données sensibles. Des règles particulières s'appliquent donc :

- Un besoin spécifique

Le recours à un dispositif biométrique doit avant tout répondre à un vrai besoin qui devra être démontré par écrit dans l'étude d'impact sur la vie privée que la CNIL recommande d'effectuer avant la mise en œuvre d'un traitement de données biométriques.
Exemple : authentification pour permettre l'accès à un lieu, une application ou un service.

- Liberté d'y recourir ou de choisir un dispositif alternatif

L'utilisateur doit pouvoir librement choisir d'utiliser le dispositif biométrique ou non. Il est nécessaire de recueillir son consentement.

Pour plus de détails sur le sujet, cliquez ici.

- ✓ **Géolocalisation /vidéosurveillance**

Concernant ces données, le règlement n'a pas modifié les règles déjà applicables. Seule l'obligation de déclaration préalable à faire auprès de la CNIL a été supprimée.

- ✓ **Intérim**

Dans le cas de l'intérim, l'entreprise d'intérim n'est responsable que des données liées à l'établissement des paies. L'entreprise utilisatrice gère notamment les données liées à la vidéosurveillance et aux congés.

LIENS UTILES

Règlement européen sur la protection des données personnelles

CNIL

Formulaire de collecte des données
Formulaire de désignation d'un DPO
Précisions sur la portabilité
Outils sur l'étude d'impact
Guide sur la sécurité des données personnelles
Guide du sous-traitant
Guide à destination des TPE/PME
Fiche sur la communication et vente en ligne
Fiche sur la relation client
Fiche sur la protection des collaborateurs

MEDEF

Questionnaire d'autoévaluation
Guide

CPME

Fiche pratique

CGI

Point sur le règlement européen sur les données personnelles