

# RESPECTER LA VIE PRIVÉE, PAR OÙ COMMENCER ?

## LA CHECK-LIST POUR LES TPE/PME

### Quelles informations avez-vous sur vos clients et fournisseurs ?



« J'ai un fichier de clients et de fournisseurs.  
Quelles informations puis-je inclure ? »

« Je souhaite installer des caméras de vidéosurveillance  
dans mon magasin. Quelles mesures dois-je prendre ? »

« Est-ce que je peux envoyer ma prospection commerciale  
par courrier à toutes les personnes de la région ? »

Dans de nombreuses situations, vous pouvez avoir des informations sur les personnes qui permettent de les identifier : **ce sont des données personnelles**. Il peut s'agir du nom ou prénom, du numéro de téléphone, de l'adresse postale ou de messagerie électronique, un visage et même une voix !

#### Pourquoi faire attention à ces informations ?

Au-delà du respect de la loi, qui est contrôlé par la CNIL, respecter la vie privée et les droits de personnes, c'est :

- **créer un sentiment de confiance chez vos clients ;**
- **améliorer votre efficacité commerciale ;**
- **mieux gérer votre entreprise ;**
- **éviter la perte ou l'altération des données de votre entreprise.**



#### POUR SAVOIR OÙ VOUS EN ÊTES,

complétez la check-list créée spécialement pour les TPE / PME !



Dans tous les cas, vous devez respecter le règlement général sur la protection des données (RGPD) et la loi Informatique et Libertés.

**Attention : remplir cette check-list ne garantit pas une conformité au RGPD.**

1

## J'identifie tous les fichiers de mon entreprise

(exemples : recrutement, gestion de la paye, clients, etc.)

2

## Je fais le tri dans mes fichiers

- Je note l'objectif de chaque fichier (exemple : gestion des factures, fidélisation client, etc.)
- Je fais la liste des informations que j'enregistre pour chaque fichier et je vérifie qu'elles sont toutes indispensables pour mon objectif. Dans le cas contraire, je les supprime et ne les demande plus.
- J'identifie, pour chaque fichier, qui peut avoir besoin de ces informations (employés, partenaires, prestataires...)
- J'identifie, pour chaque fichier, combien de temps je dois garder chaque type d'informations (et ne les conserve pas au-delà !)



Dès lors que vos fichiers contiennent des informations personnelles (sur vos clients ou collaborateurs par exemple), vous devez créer un fichier qui les recense : c'est le registre des activités de traitement.

### À SAVOIR

Il doit comprendre une fiche par traitement de données (exemples : une fiche pour le système de gestion client et fournisseur, une fiche pour les données utilisées pour la paie, une fiche pour la gestion des employés, etc.).

Ce fichier pourra vous être demandé par la CNIL.



### BESOIN D'AIDE ?

Un **modèle de registre simplifié** est disponible sur le site de la CNIL (profil « je suis un professionnel ») : *Rubrique Ma conformité au RGPD > Passer à l'action > Le registre des traitements*

Retrouvez des **fiches pratiques** pour communiquer et vendre en ligne, améliorer et maîtriser la relation client et protéger les données de vos collaborateurs dans le Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises (en collaboration avec Bpifrance), disponible depuis la Médiathèque du site web de la CNIL.

### 3

## Je respecte toujours l'information et les droits des personnes

- Je préviens mes clients et fournisseurs des données que je détiens sur eux
- J'indique pourquoi je collecte des données (par exemple pour gérer les inscriptions à un évènement).
- J'indique qui a accès aux données (quels types de salariés, quels partenaires).
- J'indique combien de temps les données sont conservées (ex. : un mois pour les enregistrements vidéo).



#### À SAVOIR

Indiquez ces mentions en bas de chaque formulaire, par une affiche en caisse, une confirmation par courriel...

Vous devez répondre aux demandes d'accès, de rectification, d'opposition des personnes dans un délai maximal d'un mois. Une absence de réponse peut mener à une sanction de la part de la CNIL.

Des modèles de mention sont disponibles sur le site web de la CNIL : <https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation>

### 4

## Je sécurise mes données

Les mesures de sécurité à prendre doivent être adaptées à la sensibilité des informations et aux risques. Vous ne laisseriez pas traîner vos espèces ou bijoux ! C'est la même chose pour les données personnelles, surtout celles de vos clients.

- J'adopte une bonne hygiène numérique (mise à jour de l'antivirus et des logiciels, mots de passe forts, sauvegardes régulières des données).
- Je mets mes documents sensibles dans un coffre-fort ou une armoire sécurisée dont je suis le seul à connaître la combinaison ou à en avoir la clé.
- Je sensibilise l'ensemble des salariés, et mon entourage, aux enjeux liés à la vie privée et à la sécurité des données.



#### À SAVOIR

L'ANSSI et la CPME ont publié les 12 règles essentielles pour sécuriser les équipements numériques : **Guide des bonnes pratiques de l'informatique, 12 règles essentielles pour sécuriser vos équipements numériques**

La CNIL a publié un **guide sécurité des données personnelles** :  
Rubrique *Ma conformité au RGPD* > *Passer à l'action* > *Sécurité des données*

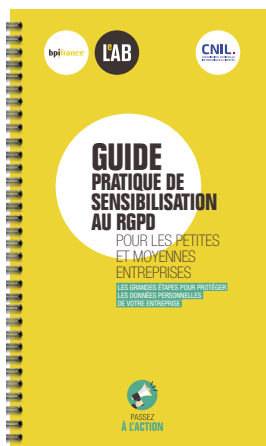
## Comment aller plus loin ?

Échangez vos questions et vos bonnes pratiques avec des entreprises voisines, votre expert-comptable ou une association !

La CNIL apporte un soutien spécifique aux organisations professionnelles et aux structures de conseil.

La CNIL et Bpifrance ont publié un guide de sensibilisation au RGPD. Il reprend les éléments de cet imprimé et va plus loin en donnant des exemples concrets.

Il est disponible gratuitement sur le site web de la CNIL.



3, PLACE DE FONTENOY - TSA 80715  
75334 PARIS CEDEX 07  
Tél. : 01 53 73 22 22