Le Règlement Général sur la Protection des Données (RGPD)

2. Les actions clés de mise en conformité

En quoi les entreprises sont-elles concernées ?

Toute organisation (entreprises, associations, organisation patronale, syndicale …) traite nécessairement dans le cadre de ses activités, des données personnelles. Elle est donc concernée et devra se mettre en conformité avec le règlement d'ici le 25 mai 2018.
La première étape de cette mise en conformité sera d'identifier les traitements de données personnelles réalisées dans le cadre de leur activité.

Exemples de traitements réalisés au quotidien

- Gestion des clients et prospects (gestion des contrats, commandes et factures, opérations de prospection, gestion des impayés, programme de fidélisation, …),
- Gestion des fournisseurs (opérations liées aux contrats, commandes, factures et règlements, …),
- Gestion du personnel (dossier professionnel, annuaire interne et organigramme, organisation des élections professionnelles, gestion des actions sociales et culturelles, mise à disposition d'outils informatiques, mise en place d'actions de formation, …),
- Gestion de la paie du personnel (calcul et paiement des rémunérations et frais, déclarations fiscales et sociales,…),
- Traitement de la comptabilité générale (tenue d'un inventaire, d'un compte d'exploitation générale, d'un bilan,…),
- Gestion de la téléphonie du personnel,
- Écoute et enregistrement des conversations sur les lieux de travail,
- Gestion des contentieux,
- Géolocalisation des véhicules des salariés,
- Système de vidéosurveillance, de vidéo protection,
- Gestion des badges sur le lieu de travail (contrôle de l'accès aux locaux, au restaurant d'entreprise, self,…).

Qu'entend-on par la protection des données à caractère personnel ? les 6 règles d'or à respecter par l'entreprise

Les données à caractère personnel collectées par l'entreprise doivent respecter les principes suivants :

1. Loyauté, transparence et légalité du traitement

Cela se traduit par l'information des personnes sur le traitement de leurs données personnelles. Ils doivent être informés de ce que l'entreprise fait de leurs données personnelles.

2. Limitation des finalités du traitement

C'est-à-dire qu'il est interdit de détourner l'objectif initial du traitement : un fichier de paie ne doit servir qu'à la paie.

3. Minimisation des données

C'est-à-dire qu'il est interdit de collecter des données qui ne sont pas nécessaires au regard des objectifs du traitement : ex : demander le signe astrologique d'un client.

4. Exactitude

C'est-à-dire qu'il est obligatoire que les données soient exactes et tenues à jour : ex : changement de RIB d'un salarié

5. Limitation de la conservation des données

Cela se traduit par une détermination systématique d'une durée de conservation des données personnelles au moment de leur collecte et d'une évaluation de la nécessité de conserver ou non cette donnée au terme de cette durée tout en respectant le Code du travail, le Code du commerce par exemple.

6. Intégrité et confidentialité des données

Cela se traduit par la mise en œuvre d'une politique de sécurité appropriée et adaptée aux risques.

Qui est en charge de la protection des données personnelles ?

Identification des principaux acteurs – répartition des responsabilités

Le responsable de traitement :

Au regard des textes, c'est le dirigeant de l'entreprise qui est légalement considéré comme responsable de la protection des données personnelles de citoyens européens. (loi Informatique et Libertés de 1978, RGPD). Dans ces textes, le dirigeant est considéré comme un **responsable de traitement** dès lors qu'il :

- détermine les finalités et les moyens de traitement.
- décide de mettre en œuvre le traitement et en définit les modalités.
- Il est juridiquement responsable de la conformité du traitement et veille au respect des obligations.

Le sous-traitant :

Le sous-traitant est la personne, le service ou l'entreprise qui traite des données personnelles pour le compte du responsable de traitement. Il peut s'agir d'un prestataire de services (par exemple, un éditeur de logiciels, prestataires informatiques, plateformes numériques,…).

Le sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et en matière de conformité. **Il a notamment une obligation de conseil auprès du responsable de traitement pour la conformité à certaines obligations du règlement** (étude d'impact éventuelle, failles de sécurité, destruction de données, contribution aux audits). Il peut donc être également sanctionné en cas de non-respect.

Quelle démarche à engager pour garantir la protection des données personnelles ?

Une démarche en 3 étapes

Porter la démarche au plus haut niveau de la gouvernance de l'entreprise.
Désigner un « pilote » de la démarche même lorsque la désignation d'un Délégué à la Protection des données (DPD) n'est pas obligatoire.

1. État des lieux

- Nomination d'un pilote si nécessaire
- Rencontre avec les différentes fonctions supports de l'entreprise
- Audit des pratiques des traitements (papiers et électroniques), des documents existants (formalités préalables, formulaires d'information, recueil de consentement, durée de conservation,…)
- Audit du système d'information

2. Diagnostic

- Bilan des conformités et non conformités
- Identification des écarts réglementaires
- Analyse globale des risques et priorisation des mises en conformité

3. Plan d'action

- Organiser la mise en conformité (documents d'information sur les droits des personnes,…)
- Sensibiliser les collaborateurs à la protection des données
- **Documenter la conformité (registre des traitements,…)**

Comment se mettre en conformité avec le RGPD ?

Le registre des traitements

La tenue d'un **registre des traitements** est l'une des obligations les plus importantes imposées par le RGPD. Le registre des traitements prouve que l'on est bien dans le respect de la loi.

Le Règlement Général sur la Protection des Données prévoit une dérogation pour les organisations de moins de 250 employés en ce qui concerne la tenue d'un registre de traitements de données personnelles. Toutefois, une liste des traitements de données personnelles est fortement recommandée, notamment lorsque les traitements sont susceptibles de comporter des risques pour les droits et libertés des salariés ou des données sensibles (N° SS, casier judiciaire, etc.).

Ce sera le registre des traitements qui va prouver la conformité de l'organisation avec le RGPD.

Quels sont les éléments que doit comporter le registre des traitements ?

Tenir un registre des traitements en tant que responsable de traitement (RT) et en tant que sous-traitant (ST) comporte les points suivants :

Registre du RT	Registre du ST
➢ Coordonnées du RT et le cas échéant du pilote désigné ➢ Finalités, catégories de personnes concernées et de données personnelles ➢ Catégories de destinataires (y compris ceux situés hors UE) ➢ Transferts de données (le cas échéant) ➢ Délais prévu pour l'effacement des données ➢ Mesures de sécurité	➢ Coordonnées du ST, RT et le cas échéant du pilote désigné ➢ Catégories de traitements ➢ Transferts de données (le cas échéant) ➢ Mesures de sécurité.

Ce qu'il faut retenir

A compter du 25 mai, les entreprises n'auront plus, sauf exception, à déclarer leurs traitements de données personnelles à la CNIL. Mais elles devront, pour assurer leur conformité avec les exigences du RGPD :

- Lister les traitements de données personnelles en identifiant leur finalité, le support associé et les destinataires,
- Les répertorier dans un registre dédié ou sur une liste de traitements de données personnelles,
- Lister les actions de conformité à mener en priorisant les plus sensibles,
- Sécuriser les traitements les plus sensibles en effectuant une analyse d'impact sur la protection des données,
- Revoir l'organisation interne en mettant à jour les mentions d'information, revoir la règles d'archivage, rappeler certaines bonnes pratiques aux collaborateurs,
- Documenter et tracer les moyens mis en œuvre pour garantir la protection des données.

Sanctions

Cadre légal actuel	Règlement européen
➢ **Rappel : pouvoirs de contrôle de la CNIL** - Contrôle sur place - Contrôle sur pièces - Contrôle sur convocation, - Contrôle en ligne ➢ **Sanctions** - Sanctions administratives – ex. sanctions financières pécuniaires jusqu'à 3 000 000 € (loi pour une République numérique), - Sanctions pénales, - Risques de l'image/commercial - Risque de contentieux social/commercial	➢ **Rappel : pouvoir des autorités de contrôle** ➢**Pouvoirs de contrôle (enquête)** - Mener des enquêtes sous forme d'audit - Procéder à un examen des certifications - Accéder aux informations et aux locaux du RT et du ST ➢**Pouvoirs de sanctions** ➢**Renforcement des sanctions administratives :** - Jusqu'à 20 M€ ou 4% du CA annuel global - Simple avertissement ➢ **Sanction pénale applicable selon la législation nationale**