Concrètement, qu'est-ce qu'une entreprise doit faire ?

1. **Documenter et être en mesure de démontrer sa conformité** en cas de contrôle de la CNIL ou en cas de réclamation d'une personne dont les données personnelles sont collectées ou utilisées. Cela signifie :

   - ***Plus de déclaration à la CNIL*** : vous n'avez plus besoin d'informer préalablement la CNIL de l'existence d'un traitement.
   - ***Désignation d'un DPO ('Data Protection Officer')*** : vous devez nommer un délégué à la protection des données (ou *DPO*) ou désigner un référent / pilote en charge des problématiques de protection des données personnelles.
   - ***Tenue d'un registre de traitement*** : pour certaines structures, vous devez tenir un registre des traitements de données personnelles que vous effectuez dans votre entreprise ou que vous externalisez (gestion de la paie, hébergement externe des données numériques, utilisation du Cloud, utilisation d'un coffre-fort numérique…).

2. **Sensibiliser ses collaborateurs et salariés** aux problématiques et enjeux de la protection des données personnelles. Cette sensibilisation peut être faite par tous moyens (en présentiel, par la diffusion d'une note d'information, l'actualisation du règlement intérieur, la signature d'un engagement de confidentialité…).

3. **Informer les personnes concernées** de l'existence d'un traitement de leurs données personnelles et, quand cela est nécessaire, demander leur consentement.

   - ***Informer les salariés*** (annexe au contrat de travail, note interne, charte d'utilisation des outils informatiques…).
   - ***Informer les clients*** (prévoir des mentions d'information dans les mails, dans les CGU/CGV, dans les courriers, sur des formulaires de collecte… ; le cas échéant, informer oralement les interlocuteurs par téléphone).

4. **Vérifier les contrats avec ses prestataires** :

   - ***Identifier les prestataires ou partenaires qui traitent des données personnelles pour le compte de votre entreprise*** (expert-comptable, gestionnaire de paie, gestionnaire du coffre-fort numérique, hébergeur, prestataire de maintenance informatique, société de sécurité, développeur d'applications ou de logiciels…) et qui sont donc considérés comme sous-traitants au sens du RGPD.
   - ***Les informer*** par écrit (mail ou courrier) de l'entrée en application du RGPD et de leurs obligations en tant que sous-traitants.
   - ***Leur proposer d'intégrer les clauses imposées par le RGPD dans les contrats en cours***.
   - ***Modifier les modèles de contrat pour y intégrer les clauses contractuelles imposées par le RGPD***.

5. **Assurer la sécurité de ses traitements :**

   - ***Veiller à tout le moins à respecter les mesures élémentaires préconisées par la CNIL dans son guide pratique***.

   ➢ *Sécuriser les fichiers :*

- *Sécuriser l'accès au fichier (gestion des droits d'accès)*
- *Mettre un mot de passe à l'ouverture du fichier s'il contient des données sensibles (données de santé ou numéro de sécurité sociale par exemple)*
- *Mise en place de logs pour être en mesure de détecter les intrusions en cas de vol de fichiers, d'accès non autorisé, de fuite de données…*
- *Avoir une sauvegarde du fichier ou de ses données pour être en mesure de restaurer un fichier modifié ou supprimé*

➢ *<u>Sécuriser les smartphones ou tablettes</u> :*
- *Mettre un code de verrouillage de l'appareil*
- *Crypter les tablettes Android*
- *Utiliser un MDM (Mobile Device Management) qui permet de gérer les tablettes ou smartphones à distance afin d'effacer les données en cas de perte / vol du terminal*

➢ *<u>Sécuriser les ordinateurs fixes ou portables</u> :*
- *Mettre un mot de passe individuel sur les ordinateurs*
- *Crypter l'ordinateur portable s'il contient des fichiers ayant des données personnelles / confidentielles*
- *Avoir un antivirus à jour*
- *Mettre régulièrement à jour le système d'exploitation, les outils, logiciels ou applications utilisés*

- ***Mettre en place un processus de notification des violations de données personnelles*** (incidents de sécurité ayant impacté les données personnelles). A compter d'aujourd'hui, il faut notifier à la CNIL tous les incidents de sécurité impactant les données personnelles (accès non autorisé, fuite volontaire ou accidentelle de données, indisponibilité involontaire ou anormale des données, suppression ou modification intentionnelle ou accidentelle des données…) lorsqu'il existe un risque pour les personnes concernées (par exemple en cas de fuite de données bancaires).

6. **<u>Respecter les droits des personnes concernées</u>** d'accéder aux données les concernant, de s'opposer à un traitement, de demander l'effacement de leurs données… Cela implique de mettre en place un processus de gestion des réclamations des personnes concernées pour leurs données personnelles.