SENSIBILISATION DES ORGANISATIONS DE LA CGT AUX OBLIGATIONS DU R G P D

Administration confédérale – mars 2021

QU'EST-CE QUE LE RGPD ?

Le sigle RGPD signifie « **Règlement Général sur la Protection des Données** ».

Le RGPD est un Règlement européen applicable **depuis le 25 mai 2018** pour toutes les entreprises, organismes, associations et entités traitant des données personnelles.

Une **donnée personnelle** est une information permettant d'identifier une personne : un nom, une adresse mail, un numéro de matricule, un numéro de téléphone, une photo...

Certaines données sont considérées comme « sensibles » car leur révélation publique sans le consentement de la personne peut présenter des risques. C'est notamment le cas de **l'appartenance syndicale**, une donnée collectée par la CGT et ses entités.

POURQUOI LE RGPD ?

Ce règlement a pour objectif de définir un cadre juridique permettant de développer les activités numériques en se fondant sur la **confiance des personnes**.

➔Le RGPD donne ainsi une réponse à **trois objectifs majeurs** : renforcer les droits des personnes, responsabiliser les acteurs des traitements de données et développer les pouvoirs des autorités de contrôle.

➔En France, c'est la CNIL qui est en charge de faire respecter le RGPD, et elle réalise des contrôles **chaque année** en se déplaçant dans les locaux des organismes, ou en demandant des documents par courriel.

QUELLES SANCTIONS EN CAS DE NON-RESPECT ?

Le RGPD s'applique à la CGT et l'ensemble de ses organisations depuis le 25 mai 2018. Chaque entité doit donc respecter les obligations et principes du RGPD, sous peine d'être sanctionnée par la CNIL.

!

- Ne pas répondre aux obligations du RGPD, c'est prendre le risque **d'entacher sa réputation** auprès de l'opinion publique. Il faut voir ce Règlement comme une opportunité de créer de la confiance avec les adhérents mais aussi les non-adhérents.
- Les organisations doivent pouvoir démontrer à tout moment leur **conformité** à la réglementation.
- Ne pas respecter le RGPD, c'est aussi s'exposer à de **lourdes amendes**.

CHACUN ACTEUR DU TRAITEMENT DES DONNÉES

Chaque responsable ou collaborateur qui agit pour son organisation contribue activement et quotidiennement à la mise en œuvre des traitements des données de l'organisation pour laquelle il travaille,

- Collecte des données.
- Copie des données.
- Transmission des données.

- Conservation des données.
- Archivage des données.
- Suppression des données.

Chaque collaborateur doit ainsi participer à la protection de la vie privée des personnes dont les données sont traitées.

Quels sont les points de vigilance ?

Mails reçus et envoyés

Documents papiers (fiches, bulletins, impressions de mails…)

Fichiers adhérents

Dossier du personnel

Tableurs Excels (listes de personne, suivi de demandes…)

Listes de diffusion

Liste des destinataires du journal de l’organisation

Suivi des stagiaires des formations syndicales

QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

Identification directe ou indirecte : peu importe !

Le RGPD s'applique dans les mêmes conditions.

➜ C'est toute information se rapportant à une **personne physique**. Elle peut identifier une personne directement ou indirectement.

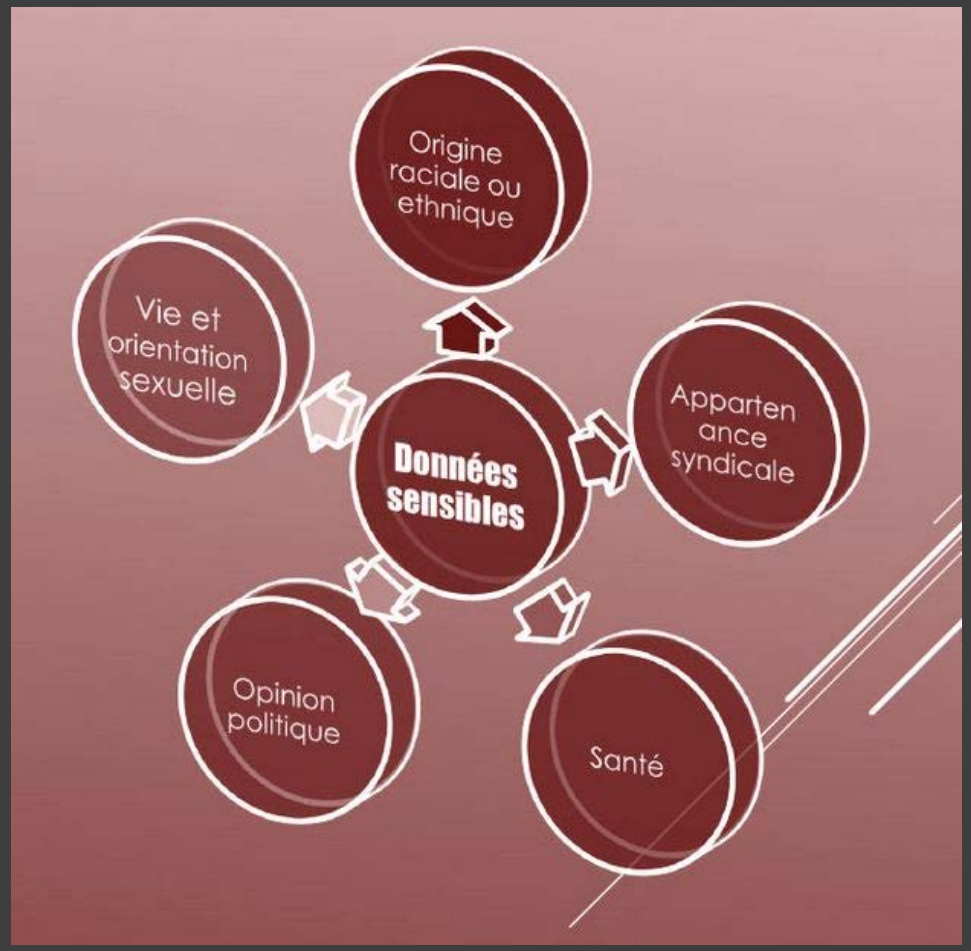
➜ Une donnée qui identifie **directement** une personne est une donnée qui se suffit à elle-même : un nom/prénom, une adresse mail nominative, une photo…

➜ Une donnée qui identifie **indirectement** a besoin d'être croisée avec d'autres données pour identifier. Par exemple, en croisant le syndicat d'appartenance et l'adresse postale personnelle, je suis en mesure de déduire l'identité de la personne.

LES DONNÉES DITES « SENSIBLES »

C’est une information personnelle qui bénéficie d’une protection spécifique. Son traitement peut engendrer des risques importants pour les droits et libertés de l’individu concerné.

Le traitement des données sensibles est interdit, sauf exceptions particulières prévues par le RGPD (art. 9).



RESPECTER LA FINALITÉ DE VOS TRAITEMENTS

Règle n°1 :

La finalité d'un traitement est l'objectif pour lequel les données personnelles sont collectées et traitées, il n'est pas possible de traiter des données sans but déterminé en amont.

Une fois que le traitement possède une finalité, cette dernière constitue un cadre : il n'est pas possible par principe de traiter les données en dehors de cette finalité.

En pratique :

- Je traite les données des adhérents pour gérer leur adhésion et le paiement de leurs cotisations. C'est un traitement avec une finalité.
- Je traite les données des adhérents pour leur envoyer des lettres d'information. C'est un autre traitement avec une autre finalité.
- Ces deux traitements sont indépendants l'un de l'autre, et chacun possède ses propres règles. Dans cet exemple, gérer les adhésions n'ouvre aucun droit à envoyer des lettres d'information à l'adhérent.
- Seules les données nécessaires pour répondre à l'objectif identifié sont collectées.

INFORMER LES PERSONNES CONCERNÉES

Règle n°2 :

C'est le principe de transparence. Il est nécessaire d'informer les personnes de l'identité du responsable de traitement, de l'usage qui sera fait de leurs données, ou encore des droits dont ils disposent sur leurs données.

L'information doit être délivrée dans un format compréhensible, concis et facilement accessible.

En pratique :

➜ Lorsque vous traitez les données des personnes, elles doivent être informées des modalités de ce traitement (identité du RT, durée de conservation, droits…)

➜ Il est possible d'informer la personne en centralisant ces informations dans un document accessible. Dans le cas d'une page web, le lien URL vers cette page peut être communiqué pour rediriger la personne.

➜ Par exemple : « Votre adresse mail est traitée afin de recevoir nos lettres d'information. Pour en savoir plus sur la protection de vos données et vos droits, cliquez ici [lien URL vers la page dédiée]. »

➜ Les personnes dont les données sont traitées ont des droits : accès, rectification, effacement, réclamation…

ATTRIBUER UNE BASE LÉGALE POUR CHAQUE TRAITEMENT

Règle n°3 :

Pour qu'un traitement soit mis en œuvre, il doit être licite, c'est à dire qu'il doit avoir une base légale.

C'est le fondement juridique qui autorise légalement le traitement à exister, c'est ce qui donne le droit au RT de traiter les données personnelles.

Chaque traitement possède une base légale. Il en existe 6 différentes, mais certaines sont plus communes que d'autres.

En pratique :

➜ Le consentement de la personne : cette base légale permet par exemple de pouvoir envoyer à la personne une lettre d'information par mail.

➜ L'exécution d'un contrat : cette base légale permet par exemple de pouvoir gérer les adhérents présents dans COGITIEL (via l'acceptation des Conditions Générales d'Utilisation).

➜ Le respect d'une obligation légale : cette base légale permet par exemple à la CGT et ses entités de contacter les salariés électeurs pour les sensibiliser à l'importance du scrutin et mener une campagne électorale (élection TPE).

DÉFINIR UNE LIMITE DE DURÉE DE LA CONSERVATION DES DONNÉES

Règle n°4 :

Les données sont collectées pour une durée limitée dans le temps.

En pratique :

Les données sont recueillies et conservées pour répondre à un objectif identifié. Une fois cet objectif atteint, si les données n'ont plus d'utilité, elles doivent être supprimées.

Exemple 1 :

Les données relatives aux candidats sont conservées pour les besoins du processus de recrutement. À son terme, si le candidat n'est pas retenu, les données n'ont a priori plus d'utilité.

Exemple 2 :

Les dossiers du personnel sont conservés pour les besoins de la gestion de leur situation administrative. À la suite d'un départ, les données doivent être archivées et conservées dans un endroit dont l'accès est restreint.

PRENDRE LES MESURES POUR GARANTIR LA SÉCURITÉ DES DONNÉES

Règle n°5 :

Les données sont utilisées de manière sécurisée, de façon à ce que seules les personnes devant en connaître, y aient accès. Adopter des mesures de sécurité, c'est également garantir qu'elles ne soient ni modifiées, ni détruites.

En pratique :

Les mesures doivent être appropriées en prenant notamment en compte le contexte et les finalités du traitement, ainsi que les risques pour les personnes.

Exemple 1 :

Tout collaborateur n'a pas vocation à accéder aux données relatives à la situation administrative des salariés de l'organisation.

Exemple 2 :

Les accès aux bureaux doivent être restreints (badge, clé) tout comme les accès aux outils informatiques (identifiant, mot de passe).

LE CONTRÔLE DE LA CNIL

La Commission nationale de l'informatique et des libertés (CNIL) peut effectuer des vérifications auprès de tout organisme traitant des données à caractère personnel.

Dans le cadre d'un contrôle, la CNIL peut:

-s'entretenir avec le personnel de l'organisation : responsables, service informatique, service RH, médical, financier...

-prendre copie de toute pièce, numérique ou papier, utile à sa mission : notes de service, contrats avec des prestations, notes d'information aux personnels, politique de confidentialité, charte informatique, organigramme, contenu des dossiers papiers…

- Accéder aux outils informatiques et aux bases de données pour opérer des extractions et des requêtes.

LES OBLIGATIONS DU DPO

L'organisation doit désigner un DPO (Data Protection Officier – en français Délégué à la protection des données). C'est obligatoire dès lors que l'organisme traite des données sensibles. L'appartenance syndicale d'une personnes est une donnée sensible.

Quel profil ?

- Le DPO doit avoir une certaine connaissance juridique du RGPD tout en maîtrisant les enjeux liés aux nouvelles technologies et à l'informatique.
- Le DPO ne peut pas exercer des fonctions de direction, ni participer à la création des traitements.

Quelle mission ?

- Être le point de contact avec les personnes dont les données sont traitées.
- Contrôler le respect du RGPD.
- Accompagner et conseiller les responsables sur la protection des données.
- Responsabiliser les acteurs et faire en sorte que chacun soit concerné par les questions de protection des données.

LES MISES EN DEMEURE ET SANCTIONS DE LA CNIL

La publicité de la mise en demeure et/ou de la sanction de la CNIL peut avoir de lourdes conséquences sur l'image publique de l'organisation.

Les sanctions financières peuvent être très importantes.

Au regard des manquements constatés lors des contrôles (nombre, gravité…) la CNIL peut :

- Adopter une mise en demeure à l'encontre du responsable du traitement :
  - Injonctions de la CNIL et mise en conformité dans un délai donné.
  - Publicité selon le contexte.
- Prononcer une sanction administrative :
  - Publicité selon le contexte.
  - Amende administrative (jusqu'à 20 millions d'euros).

Récapitulatif des principes généraux

- Les données ne sont données que pour **répondre à un objectif préalablement déterminé et défini**.
- Seules les données **nécessaires pour répondre à l'objectif déterminé** sont recueillies.
- Les données sont **conservées pour une durée limitée dans le temps** en fonction de mes besoins.
- Des **mesures permettant de garantir la sécurité et la confidentialité** des données.
- Les personnes dont je traite les données doivent être **informées de la façon dont elles sont utilisées et de leurs droits**.
- Les **droits des personnes doivent être respectés,** toute demande devant recevoir une réponse.