E31 - DROIT DES DONNÉES PERSONNELLES

L'informaticien et les données protégées

LES OUTILS NUMÉRIQUES SONT AUTANT DE CANAUX OÙ PEUVENT CIRCULER LES INFORMATIONS PERSONNELLES, MAIS AUSSI DES DONNÉES CONFIDENTIELLES RELATIVES À L'ENTREPRISE.

Les Échos

INTRODUCTION - DÉFINITIONS

Donnée : c'est **un élément brut**, sans contexte, qui n'a **pas été encore interprété**.

Une donnée brute peut prendre différents aspects. Cela peut être des données numériques, textuelles, ou un mélange de texte et de chiffres, mais aussi un tableau, un graphique**…**

Information : c'est une ou plusieurs données traitées, données qui auront été analysées et auront suivi un processus résultant en une information.

Donnée à caractère personnel : Pour être qualifiée de **donnée à caractère personnel**, l'**information** collectée doit permettre l'identification, directe ou indirecte de la personne visée.

Les DCP sont protégées par divers instruments juridiques notamment la loi Informatique, fichiers et libertés de 1978 et le Règlement général sur la protection des données ou RGPD.

PLAN

I. **La protection des données à caractère personnel**

A. Les données personnelles - Les données sensibles

B. Le RGPD - La CNIL

C. Le « RESPONSABLE » de traitement

D. Le traitement des données personnelles

II. **La protection de l'information et du système d'information**

A. Secret professionnel, confidentialité, discrétion professionnelle

B. Secret des affaires

C. Atteinte aux STAD

I. LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

A. LA NOTION DE « DONNÉES PERSONNELLES »

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ».

Une personne peut être identifiée :

- **directement** (exemple : nom, prénom)
- **ou indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- **à partir d'une seule donnée** (exemple : numéro de sécurité sociale, ADN)
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

B. LE RGPD – LA CNIL

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES PERSONNELLES

LA COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉ

QUI EST CONCERNÉ PAR LE RGPD ?

- **Le RGPD s'adresse à toute structure privée ou publique effectuant de la collecte et/ou du traitement de données**, et ce quel que soit son secteur d'activité et sa taille. Le règlement s'applique à **tous les organismes établis sur le territoire de l'Union Européenne**, mais aussi à tout organisme implanté hors de l'UE mais dont l'activité cible directement des résidents européens.

- À noter que le RGPD concerne également **les sous-traitants**, c'est-à-dire toute structure qui traiterait ou collecterait des données personnelles pour le compte d'une autre entité.

ÉVOLUTION DES DROITS DES PERSONNES AVEC LE RGPD

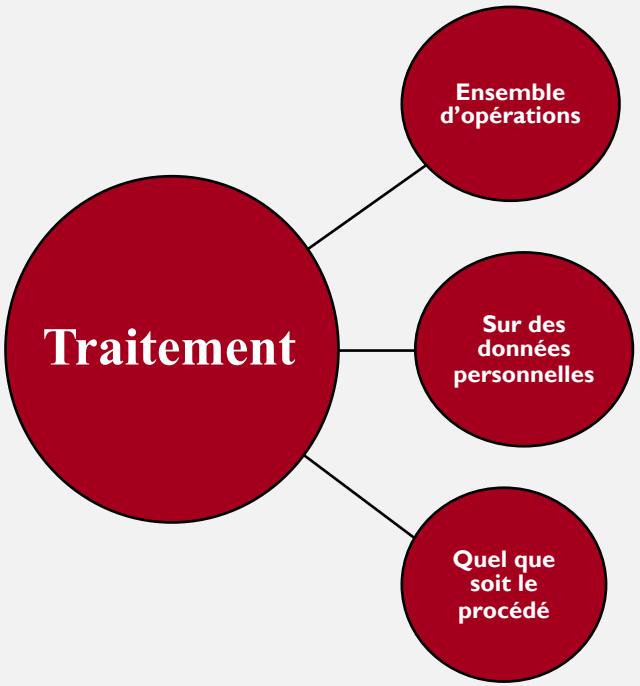
Mentions d'information obligatoires :

- Vis-à-vis des visiteurs, exposants
- Vis-à-vis des collaborateurs
- Vis-à-vis des candidats au recrutement
- Vis à vis des utilisateurs du site Internet (si collecte des données sur le site Internet)
- Vis-à-vis plus généralement de tous contacts personnes physiques dont les données seraient traitées (prospects, fournisseurs, relations professionnelles, visiteurs, etc.)

C. QU'EST-CE QU'UN « TRAITEMENT » DE DONNÉES PERSONNELLES ?

Cette notion est également très large.

Traitement de données personnelles
Article 4, 2) RGPD



- Collecte
- Enregistrement
- Conservation
- Consultation
- Diffusion
- Effacement
- Transfert UE / hors UE

D. QU'EST-CE QU'UN « RESPONSABLE » DE TRAITEMENT ?

- **Responsable de traitement:** celui qui détermine les finalités et les moyens du traitement

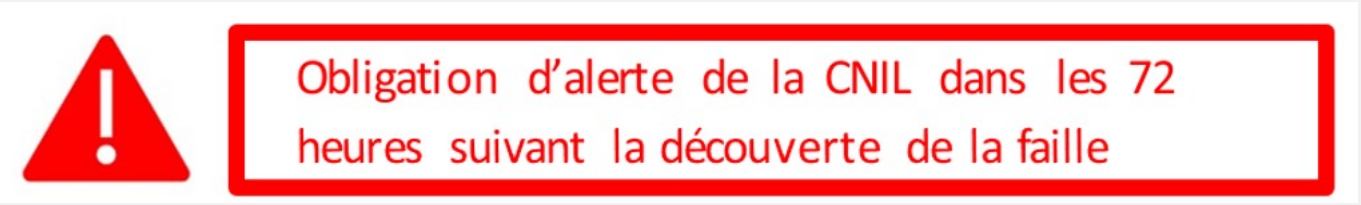
- **Cotraitance:** les coresponsables de traitement sont conjointement tenus de respecter les obligations relatives au traitement.

- **Sous-traitance :** Le sous-traitant agit pour le compte du responsable de traitement. Il doit fournir les garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles nécessaires pour la conformité au RGDP et la protection des droits des personnes.

OBLIGATION DE SÉCURITÉ DE TRAITEMENT

- Obligation à la charge du **Responsable du traitement** et du **sous-traitant**
- Mise en œuvre des **mesures techniques et organisationnelles** appropriées pour garantir un niveau de sécurité adapté au risque, telles que : pseudonymisation, anonymisation, garantir la confidentialité des systèmes de traitement, permettre de rétablir la disponibilité/accès aux données si incident physique ou technique

Si violation des données :



LES OBLIGATIONS DU RGPD : ANALYSE D'IMPACT (« PRIVACY IMPACT ASSESSMENT – PIA »)

- **Obligatoire pour les traitements susceptibles d'engendrer un « risque élevé pour les droits et libertés », et en particulier s'il y a** :
  - Profilage,
  - Traitement à grande échelle de données sensibles,
  - Surveillance systématique et à grande échelle de zones accessibles au public.
- **Les Autorités de protection des données peuvent déterminer les catégories de traitements nécessitant une étude d'impact.**

LES 4 GRANDES MISSIONS DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

1. Conseiller et accompagner l'organisme ;
2. Contrôler l'effectivité des règles en matière de protection des données ;
3. Être le point de contact de l'organisme sur les sujets RGPD ;
4. Assurer la documentation des traitements de données.

SANCTIONS PÉCUNIAIRES EN CAS DE NON-CONFORMITÉ À LA RÈGLEMENTATION

- **Amende administrative** prononcée par l'autorité de contrôle (la CNIL)
- Le montant des **sanctions pécuniaires** peut s'élever **jusqu'à 20 millions d'euros** ou dans le cas d'une entreprise **jusqu'à 4 % du chiffre d'affaires annuel mondial**. Ces sanctions peuvent être rendues publiques.
- **+ sanctions pénales possibles** (art 226-16 et suivants du code pénal : => 5 ans d'emprisonnement et 300 000€ d'amende

Source: CNIL

II. LA PROTECTION DE L'INFORMATION ET DU SYSTÈME D'INFORMATION

A. SECRET PROFESSIONNEL, CONFIDENTIALITÉ, DISCRÉTION PROFESSIONNELLE

TOUTES LES DONNÉES, MÊME À CARACTÈRE NON PERSONNELLES SONT PROTÉGÉES

- **Si violation du secret professionnel** : art 226-13 du Code pénal

Peine : => 1 an de prison et 15 000€ d'amende

- **Si atteinte aux STAD** : art 323-1 et suivants du Code pénal

- Accès frauduleux : => 2 ans de prison et 60 000 d'amende
- Accès + suppression, modification : => 3 ans de prison et 100 000€ d'amende
- Si accès + suppression, modification à l'encontre d'un STAD de DCP mis en œuvre par l'Etat :

  => 5 ans de prison et 150 000€ d'amende

- **Si les données sont à caractère personnel** :

Infraction à la loi Informatique et Libertés : => 3 ans de prison et 100 000€ d'amende

Assimilé à un homicide involontaire, infiniment plus sanctionné

LE SECRET PROFESSIONNEL

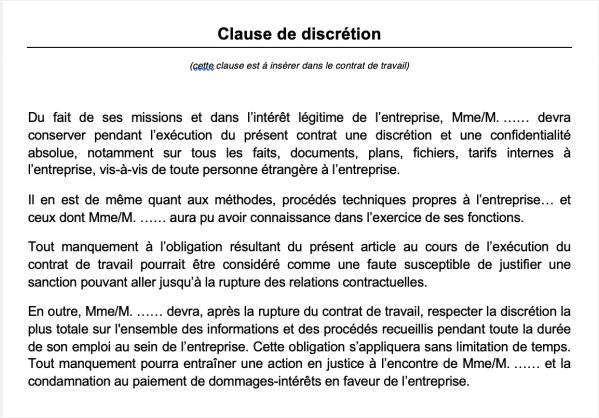
Le **secret** professionnel tel **qu**'il apparaît à l'article **226-13** du Code pénal concerne toute personne **qui**, dans son état ou sa profession, ou en raison d'une fonction ou d'une mission temporaire, a reçu des informations auxquelles la loi accorde le caractère de **secret**.

Les informations couvertes par le secret professionnel **ne sont définies par aucun texte de loi mais 3 critères :**

- **révélation d'une information qui n'était pas connue avant**
- **à caractère secret**
- **par un professionnel**

DISCRÉTION PROFESSIONNELLE ET CONFIDENTIALITÉ

Obligation générale de discrétion et de confidentialité à l'égard des informations auxquelles le salarié a accès au sein de l'entreprise et dans le cadre de ses fonctions : secret de fabrication, secret commercial, documents financiers, paye, information sur la clientèle…



Clause de discrétion

(cette clause est à insérer dans le contrat de travail)

Du fait de ses missions et dans l'intérêt légitime de l'entreprise, Mme/M. …… devra conserver pendant l'exécution du présent contrat une discrétion et une confidentialité absolue, notamment sur tous les faits, documents, plans, fichiers, tarifs internes à l'entreprise, vis-à-vis de toute personne étrangère à l'entreprise.

Il en est de même quant aux méthodes, procédés techniques propres à l'entreprise… et ceux dont Mme/M. …… aura pu avoir connaissance dans l'exercice de ses fonctions.

Tout manquement à l'obligation résultant du présent article au cours de l'exécution du contrat de travail pourrait être considéré comme une faute susceptible de justifier une sanction pouvant aller jusqu'à la rupture des relations contractuelles.

En outre, Mme/M. …… devra, après la rupture du contrat de travail, respecter la discrétion la plus totale sur l'ensemble des informations et des procédés recueillis pendant toute la durée de son emploi au sein de l'entreprise. Cette obligation s'appliquera sans limitation de temps. Tout manquement pourra entraîner une action en justice à l'encontre de Mme/M. …… et la condamnation au paiement de dommages-intérêts en faveur de l'entreprise.

B. LE SECRET DES AFFAIRES

- **Loi du 30 juillet 2018 sur la protection du secret des affaires.**
- Pour être protégée au titre du **secret des affaires,** une information doit remplir trois conditions :

  - ne pas être « *généralement connue ou aisément accessible* »,
  - revêtir « *une valeur commerciale, effective ou potentielle* »
  - faire l'objet de « *mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret* ».

C. ATTEINTE À UN STAD

L'accès frauduleux à un STAD est défini par **l'article 323-1 du Code pénal** comme étant :

« *Le fait* ***d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données***. ».

L'auteur de cette infraction est puni de **2 ans d'emprisonnement** et **30 000 euros d'amende**. Dans le cas où il résulte de cette infraction une suppression ou une modification des données du système, la peine est **de 3 ans d'emprisonnement** et **45 000 euros d'amende**.

Une question pour finir !

Webmaster ou responsables de sites :

comment répondre aux demandes de suppression de données personnelles publiées sur votre site ?

Merci pour votre attention ☺

Avez-vous d'autres questions ?