INCIDENCES PRATIQUES DE L'ENTREE EN APPLICATION DU RGPD EN MATIERE DE RESSOURCES HUMAINES

Règlement UE 2016/679 du 27 avril 2016

Pour s'adapter aux nouvelles réalités du numérique, l'Union Européenne (UE) a adopté le 27 avril 2016 le Règlement Général sur la Protection des Données personnelles (**RGPD**).

Les entreprises de l'UE devront respecter les règles posées par le RGPD dès le 25 mai 2018, puisque les règlements européens sont d'applicabilité directe.

Un projet de loi a par ailleurs été présenté au Conseil des Ministres le 13 décembre 2017 pour adapter la législation française au RGPD.

L'entrée en application du RGPD aura de nombreuses conséquences sur la vie des entreprises, notamment en matière de ressources humaines.

actance
société d'avocats

❖ Une responsabilisation des entreprises…

- Le RPGD consacre un **changement complet de logique** en ce qui concerne la protection des données personnelles, en mettant l'accent sur la **responsabilisation des entreprises (principe d'« *accountability* »).**

- Ce changement de logique se traduit par:
  - la suppression de la plupart des formalités déclaratoires auprès de la CNIL;
  - le remplacement de ces formalités par des actions internes à l'entreprise comprenant notamment **la tenue d'un registre des activités de traitements mis en œuvre dans l'entreprise et la réalisation, dans certains cas, d'une analyse d'impact.**

❖ …associée à des sanctions renforcées

- Le RGPD renforce les sanctions encourues par les entreprises en cas de non respect des règles sur la protection des données personnelles.

- Ces sanctions pourront atteindre jusqu'à **20 millions d'euros ou 4% du chiffre d'affaires mondial.**

→ Il est donc nécessaire de profiter des prochains mois pour se mettre en conformité avec le RGPD.

❖ Comment procéder pour préparer l'entrée en application du RGPD?

La CNIL a publié un guide recensant 6 étapes qui permettront aux entreprises de se préparer à l'entrée en application du RGPD:

1) la désignation du **Délégué à la Protection des données** (*voir page suivante*)

2) un **recensement des différents traitements de données personnelles** mis en œuvre dans l'entreprise
   → **au niveau RH**, il peut notamment s'agir des systèmes de badgeage, de la gestion des recrutements et de la paie, de l'organisation des élections professionnelles, etc…

3) la priorisation des actions à mener à l'aide du **registre des activités de traitement**.

4) la réalisation d'une **étude d'impact sur la protection des données** pour les traitements de données personnelles qui ont été identifiés comme étant **susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées**.

5) **l'organisation des processus internes**, notamment pour traiter les réclamations et demandes et anticiper les violations de données.

6) la **documentation de la conformité**.

❖ Obligation de désigner du Délégué à la Protection des Données (DPD) pour certaines entreprises

➢ Le DPD aura pour mission de contrôler le respect du RGPD dans l'entreprise et de coopérer avec la CNIL.

➢ **Sa désignation est obligatoire**, quel que soit l'effectif de l'entreprise, si l'entreprise rentre dans un des **3 cas suivants**:

- Elle est une **autorité ou un organisme public;**
- Ses **activités de base** l'amènent à réaliser un **suivi régulier** et **systématique** des personnes **à grande échelle**;
- Ses activités de base l'amènent à traiter **à grande échelle** des **données dites « sensibles »** ou **relatives à des condamnations pénales** et **infractions**.

➢ Le DPD peut être:

- Interne ou externe à l'entreprise;
- Mutualisé entre plusieurs entreprises, sous condition.

➢ **La désignation du DPD doit être anticipée et organisée dès aujourd'hui.**

→ Il convient donc de mener aujourd'hui **une analyse approfondie** pour vérifier si l'entreprise rentre dans un des 3 cas susvisés et d'en garder **une trace écrite**.

❖ La mise en place d'un registre des activités de traitement

- **Définition:** il s'agit d'un **document** qui doit comporter **les informations permettant de décrire l'ensemble des traitements de données personnelles réalisés par l'entreprise**.

- **Une obligation de mise en place à très large spectre:** le RGPD impose la mise en place d'un registre:
  - **Dans les entreprises de plus de 250 salariés;**
  - **Dans les entreprises de moins de 250 salariés** sous certaines conditions, et notamment lorsque **l'entreprise réalise un traitement de données personnelles de manière habituelle**.

  → ***La quasi-totalité des entreprises traitent de manière habituelle des données personnelles (gestion du personnel, par exemple) et devront mettre en place un registre.***

- **Contenu:** le registre doit comprendre l'ensemble des traitements de données personnelles mis en œuvre par l'entreprise. Ceci signifie qu'il doit comprendre:
  - tous les traitements qui ont déjà fait l'objet de déclarations auprès de la CNIL
  - tous les traitements qui bénéficiaient jusqu'ici de dispense de déclaration (ex: traitement de gestion de la paie)

- **Un contrôle possible:** Le registre doit être tenu à disposition de la CNIL.

❖ Quand faut-il réaliser une étude d'impact sur la vie privée des traitements?

- Pour certains traitements, la seule inscription au registre des activités de traitement ne sera pas suffisante.

- Les traitements visés sont **ceux susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques**.

  → **Exemples** de traitements concernés:
  - ✓ Traitement de **données sensibles** relatives à **l'origine raciale** ou **ethnique** ou aux **opinions politiques** et **religieuses**;
  - ✓ **Profilage**;
  - ✓ **Géolocalisation**.

- **Préalablement à la mise en œuvre de ces traitements**, le DPD ou, à défaut, l'entreprise **doit réaliser une étude d'impact sur la vie privée**.

- Un **logiciel** est **mis à disposition des entreprises par la CNIL** pour réaliser ce type d'étude.

- Si l'étude révèle un risque avéré, le **DPD devra consulter la CNIL** avant la mise en œuvre du traitement et la CNIL pourra s'opposer à ce dernier.

❖ Adapter ses procédures internes (1/2)

Les prochains mois doivent également être mis à profit pour:

➢ **Revoir les procédures internes afin de garantir la sécurité des données personnelles:**

Le RGPD impose aux entreprises de:

- mettre en œuvre des mesures « *techniques et organisationnelles* » garantissant un niveau de sécurité adapté pour les données à caractère personnel.
- notifier à la CNIL une faille de sécurité dans les 72h.

→ Nécessité de revoir les procédures internes pour garantir la sécurité et faire remonter les failles de sécurité rapidement.

❖ Adapter ses procédures internes (2/2)

Les prochains mois doivent également être mis à profit pour:

- **Se tenir informé de la publication de codes de conduite ou de certifications:**

  - **Codes de conduite:** les codes de conduites seront élaborés par des associations ou organisations d'entreprise et permettront aux entreprises y adhérant de se conformer plus facilement au RGPD.

  - **Certifications:** Les entreprises pourront obtenir des certifications délivrées par la CNIL pour 3 ans maximum.

→ La CNIL et certaines organisations syndicales de branche travaillent d'ores et déjà sur des codes de conduite et certifications.