RGPD

La nouvelle réglementation (UE) relative au traitement des données personnelles

Troyes, le 20 février 2018

Aurélien CASAUBON, Avocat associé

SF CONSEIL et associés
Vos droits, votre avocat.

Sommaire

Introduction

Contexte : la protection des données personnelles, un enjeu politique

- Une **augmentation des données personnelles collectées** en ligne
- Une **inquiétude croissante** des citoyens sur la protection de leurs données personnelles
- Une **prise de conscience** politique
- Un **morcellement législatif au sein de l'Union Européenne** et des textes peu adaptés aux nouvelles évolution technologiques, en France :
    - 1978 : Loi informatique et liberté
    - 1995 : Directive européenne (transposée en 2004).

SF CONSEIL et associés
Vos droits, votre avocat.

Introduction

Qu’est-ce que le RGPD ?

Le **Règlement Européen sur la Protection des Données (RGPD)** entrera en vigueur à l’échelle de l’Union européenne dès le **25 mai 2018.**

L’objectif de ce règlement est de créer un **cadre juridico-institutionnel** adapté aux usages de la nouvelle économie numérique. Il sera d’**application directe** mais laissera une marge de manoeuvre aux Etats membres.

En France il remplace la **“Loi Informatique et Liberté”** obsolète car pensée en fonction des **technologies des années 90**.

En France, la **CNIL sera l’autorité locale** et sera donc chargée : du contrôle, des sanctions en cas de non respect du règlement, de recueillir les plaintes relatives au non respect du règlement.

SF CONSEIL et associés
Vos droits, votre avocat.

Introduction

Le RGPD se définit autour de trois objectifs :

- **Renforcer** les droits des personnes avec notamment la création d'un droit à la portabilité des données personnelles et des dispositions propres aux personnes mineures

- **Responsabiliser** les acteurs traitant des données

- **Crédibiliser** la régulation par l'intermédiaire de sanctions dissuasives.

SF CONSEIL et associés
Vos droits, votre avocat.

I. Les apports du RGPD

1. Des définitions précises

- Qu'entend-on par données personnelles ?

« "Toutes les informations se rapportant à une personne physique identifiée ou identifiable. Identifiable directement ou indirectement via un identifiant (Nom, id, etc…) ou via des éléments propres à son identité (physique, génétique, psychique, économique, culturel ou sociale)."

- Qu'entend-on par traitement des données ?

- Qui est responsable ?

2. Un champ d'application élargi

- Une législation **protectrice des personnes physiques** ce qui exclue les données professionnelles des entreprises
- Un **impact plus vaste que les pays membres de l'UE**, puisqu'il concerne non pas leur territoire, mais leurs citoyens.

3. Une collecte des données plus encadrée

Pour être licite, la collecte des données devra répondre aux conditions suivantes :

- Légitime
- Déterminée
- Transparente
- Conservée
- Autorisée

3. Des droits reconnus aux personnes

- Droit à l'information
- Droit d'accès
- Droit de rectification et d'effacement
- Droit à la limitation du traitement
- Droit à la portabilité
- Droit d'opposition au traitement des données personnelles

II. Obligations et responsabilités du responsable du traitement des données

II. Obligations et responsabilités du responsable du traitement des données

1. Les obligations du responsable du traitement

- Sécurisation des données et des traitements
- Tenue d'un registre des activités de traitement
- Notification des violations de données personnelles
- Réalisation d'analyses d'impact
- Désignation d'un délégué à la protection des données (DPO)

SF CONSEIL et associés
Vos droits, votre avocat.

II. Obligations et responsabilités du responsable du traitement des données

Vous avez dit DPO ?

Le RGPD recommande ou impose suivant les cas la **nomination d'un Data Protection Officer (DPO)**. Il est le garant de la mise en œuvre des directives du Règlement, comme des processus et traitements déployés. Il est indépendant et est soumis au secret professionnel.

La nomination d'un DPO, remplaçant l'actuel CIL, est :

- Encouragé pour toutes les entreprises. Un DPO peut être **référent pour plusieurs organismes**

- Obligatoire pour les **organismes publics**

- Obligatoire pour les organismes dont l'activité de base consiste à collecter des **données à "grande échelle"** (la loi restant floue sur la signification du "grande échelle"...)

- Obligatoire pour les organismes collectant des **données "sensibles"** (la loi restant floue sur la signification du "sensible"...)

SF CONSEIL et associés
Vos droits, votre avocat.

II. Obligations et responsabilités du responsable du traitement des données

Vous avez dit DPO ?

- Le DPO peut être un **membre du personnel** ou un **prestataire**
- Le DPO doit posséder des **connaissances en matière de protection des données** ainsi que des **compétences organisationnelles** voire des **connaissances spécifiques** en fonction de la nature du traitement (données « sensibles »)
- Le DPO doit être **indépendant**

SF CONSEIL et associés
Vos droits, votre avocat.

II. Obligations et responsabilités du responsable du traitement des données

Vous avez dit DPO ?

Le DPO doit être capable de **conseiller les décideurs** quant au danger vis à vis de la protection des données lié à certaines décisions.

Quel est l'intérêt pour l'entreprise ?

- Conseil
- Contrôle
- Formation
- Audit

Le DPO est également le point de contact privilégié avec l'autorité locale de chaque pays.

SF CONSEIL et associés
Vos droits, votre avocat.

2. La responsabilité du responsable du traitement

Avec la suppression de la déclaration préalable, chaque entreprise peut faire l'objet d'un contrôle inopiné.

En cas de manquement, le responsable du traitement engage sa **responsabilité** sur le plan **administratif et judiciaire**.

L'avancée majeure apportée par le RGPD consiste à responsabiliser également les sous-traitants : **responsabilité solidaire**.

III. Droits de recours et sanctions

III. Droits de recours et sanctions

1. Droit à un recours juridictionnel effectif

Le RGPD prévoit un droit de recours effectif devant les tribunaux à toute personne qui considère que ses droits ont été violés dans le cadre du traitement de ses données personnelles .

Le RGPD reste flou sur la nature de la responsabilité (délictuelle ou contractuelle).

Il reste encore des interrogations relatives aux juridictions compétentes et aux lois applicables.

Le RGPD prévoit une exonération de responsabilité lorsqu'il est démontré que l'origine du dommage n'est pas imputable au responsable.

2. Les sanctions administratives

- Contrôle administratif exercé par la **CNIL** indépendamment du contrôle juridictionnel

- La CNIL pourra s'auto-saisir dans le cadre du contrôle *a posteriori* ou pourra être saisie par toute personne qui estime que ses droits ont été violés

- **Pas de sanction automatique** : l'appréciation tiendra compte de la nature et de la gravité de la violation, de sa durée ou encore de sa portée

- En cas de sanction, RGPD prévoit une **réponse graduée** (article 58).

2. Les sanctions administratives

Pour les violations les plus graves, le RGPD prévoit des amendes administratives :

- amende administrative de niveau 1 qui pourra s'élever jusqu'à 10M€ ou jusqu'à 2% du CA annuel mondial

- amende administrative de niveau 2 qui pourra s'élever jusqu'à 20M€ ou jusqu'à 4% du CA annuel mondial

Chaque amende viendra sanctionner une violation strictement énumérée par le RGPD.

Des sanctions supplémentaires pourront être prévues par les Etats pour les infractions qui ne font pas l'objet d'amendes administratives.

Conclusion

Conclusion

Ce qu’il faut retenir

Depuis plus de 20 ans, les **données des consommateurs sont utilisées** à des fins marketing **sans aucun encadrement ni repères**.

Avec le RGPD, orientation vers une **utilisation plus saine des données**.

Sur le plan business, la RGPD présente également des avantages non négligeables:

- La **confiance des utilisateurs** permettra d’avoir un taux d’acceptation plus élevé

- La **data collectée sera plus riche** car acceptée et donc plus pertinente.

SF CONSEIL et associés
Vos droits, votre avocat.