APOLLINAIRE

SOCIÉTÉ D'AVOCATS

DROIT DE L'ENTREPRISE ET CONTENTIEUX DES AFFAIRES

APOLLINAIRE société d'avocats conseille les entreprises préalablement à leurs décisions stratégiques et les assiste sur l'ensemble du territoire français à l'occasion de leurs procédures contentieuses à fort enjeu.

Grâce à son organisation et à la disponibilité de ses associés, le cabinet est à même de répondre, sans délai, aux situations d'urgence.

Chaque dossier est pris en charge, tout au long de son instruction, par un ou plusieurs associés. Les clients ont ainsi des interlocuteurs hautement qualifiés et responsables de leurs conseils.

27 juin 2018

Le règlement général sur la protection des données (RGPD)

Christophe ALLEAUME

27 juin 2018

SOMMAIRE

SOMMAIRE

RGPD

- Règlement du **27 avril 2016** relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données (entrée en vigueur : **25 mai 2018)**

- Loi du **14 mai 2018** relative à la protection des données personnelles

Loi du **14 mai 2018**

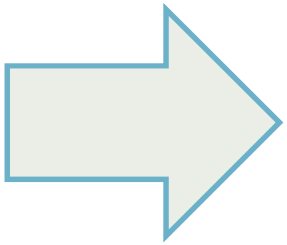
La loi est très technique et ne revient pas sur le RGPD

- Désigne la CNIL comme autorité compétente
- la CNIL peut poser des questions préjudicielles à la CJUE
- Quelques dispositions techniques sur les **données sensibles** (condamnations pénales, infractions, données de santé)
- Quelques mesures dérogatoires à l'exercice des droits des personnes si celles-ci sont nécessaires pour la **sécurité nationale**, la **défense nationale**, l'indépendance de la **Justice**, …

Les objectifs du RGPD

- Créer un cadre juridique harmonisé
  - au plan géographique
  - au plan structurel
- Renforcement des droits de l'individu
- Renforcement des obligations des responsables de traitement et des sous-traitants
- Sévérité des sanctions

Les objectifs du RGPD



Susciter la **confiance** en l'économie numérique en **protégeant** les personnes physiques vis-à-vis des traitements de leurs données à caractère personnel

Conditions d'application du RGPD

TROIS CONDITIONS CUMULATIVES :

un traitement

= Collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, …

- d'au moins une donnée à caractère personnel

= Identifiants directs : nom, prénom, photographie…

= Identifiants indirects : adresse, données de géolocalisation, identifiants en ligne, adresse IP, etc.

- un rattachement à l'Union Européenne

Principes posés par le RGPD

- Obtenir le **consentement exprès et préalable** des personnes concernées

- Respecter les principes de **licéité**, de **loyauté** et de **transparence**

Principes posés par le RGPD

Licéité - transparence - loyauté

Licéité: un traitement est licite si

1 condition au moins parmi les suivantes

❑ La personne a **consenti** au traitement

❑ le traitement est **nécessaire** à:

- **l'exécution d'un contrat**, ou

- **l'exécution d'une obligation légale**, ou

- à la **sauvegarde des intérêts vitaux** d'une personne physique, ou

- aux **intérêts légitimes** poursuivis par le responsable du traitement.

Transparence

❑ Le RGPD prévoit une liste d'informations à donner à la personne concernée en **langage clair**

✓ identité et coordonnées du responsable du traitement / délégué à la protection des données

✓ finalité(s) du traitement

✓ destinataire(s) des données

✓ durée de conservation des données

✓ droits de la personne

Droits des personnes
face au traitement de leurs données personnelles

- Droit d'accès
- Droit de rectification
- Droit à l'effacement
- Droit à la limitation du traitement
- Droit à la notification
- Droit à la portabilité des données
- Droit d'opposition
- Droit de ne pas faire l'objet d'une décision fondée sur un traitement automatisé

Obligations des établissements
traitant les données personnelles de personnes physiques

❑ L'organisme en charge du traitement et le sous-traitant sont tous deux responsables

❑ Délégué à la protection des données

❑Etre capable d'expliquer, en cas de contrôle, quelle est la politique de collecte et de conservation des données:

- dans une **relation commerciale** (commerçants – clients)
- dans une **relation avec la puissance publique** (administration – usager)
- dans une **relation de travail** (employeur – salariés)

❑ **Possibilité selon le RGPD** de prévoir un régime de faveur pour les micros et petites entreprises à la condition que la loi nationale le prévoit (possibilité non exploitée par la loi française du 14 mai 2018)

Obligations des entreprises

La responsabilité de l'organisme en charge du traitement

Responsabilité de l'organisme en charge du traitement	Coresponsabilité du Sous-traitant
❑ Il détermine les **finalités** et les **moyens** du traitement	❑ Il traite pour le compte du responsable du traitement
❑ Il est responsable du dommage qui résulterait d'une violation du RGPD	❑ Il est responsable du dommage qui résulte d'une violation : • du RGPD • des instructions « illégales » du responsable s'il les applique

Obligations des entreprises

Le délégué à la protection des données

Désignation

❑ **Obligatoire** :

✓ Organismes **public**

✓ Organismes **privés**:

- Si le traitement implique un suivi régulier, systématique, à grande échelle
- Si collecte de données sensibles

❑ **Facultative** dans les autres cas (mais pas interdite)

Missions

❑ Contrôle le respect du RGPD

❑ Informe et conseille le responsable du traitement

❑ Interlocuteur des personnes concernées par le traitement

❑ Coopère avec la CNIL

Fonction

❑ Intermédiaire

❑ Astreint au secret professionnel

Obligations des entreprises

La politique de collecte et de conservation des données

- Données à caractère personnel doivent être
  - ✓ **Adéquates**
  - ✓ **Pertinentes**
  - ✓ **Limitées** à la finalité du traitement

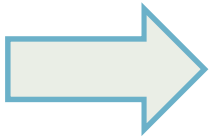
  ⇒ Sinon: conservation <u>impossible</u>

- **Durée** de conservation = limitée au **strict minimum**

Sanctions en cas non-conformité

- Amende administrative :
  - ✓ Effective
  - ✓ Proportionnée
  - ✓ Dissuasive

- Plafond maximal :
  - ✓ **20 millions d'euros**
  - ✓ ou **4%** du **chiffres d'affaires <u>mondial</u> total** de l'exercice précédent



Montant de l'amende = somme la plus élevée

Comment bien se préparer au RGPD?

❑ **Inventorier** les **données** collectées (concernant les clients, élèves, parents, fournisseurs, distributeurs, agents publics, salariés…), les **traitements**, les **finalités**

❑ **Déterminer** les **modalités** de la collecte (site internet, feuille de papier à remplir, conclusions de contrats, démarchage téléphonique…)

❑ **Vérifier le respect des principes élémentaires** du RGPD:

- ✓ Les données collectées supposent-elles un consentement ?
- ✓ Les finalités réelles de la collecte sont-elles expliquées?
- ✓ Les données collectées sont-elles nécessaires?
- ✓ Les explications données sont-elles claires?
- ✓ Comment s'exerce le droit d'accès? Etc.
- ✓ Qui efface les données (en cas de demande)?

Quelles premières actions entreprendre?

- **Réaliser** un **inventaire exhaustif** de l'ensemble des traitements effectués par l'établissement

- **Former** des membres du **personnel** chargés de veiller au respect du RGPD

- **Alerter** et **sensibiliser l'ensemble du personnel** au moyen d'une documentation interne et de formations

Merci de votre attention
et
de votre participation