Données à Caractère Personnel : les enjeux, vos obligations et vos droits face à la réforme 2016

Compte rendu effectué par la mopa suite à la conférence organisée par le Cabinet FIDAL le 30 juin 2016

En 2016, chaque organisme collecte et exploite toutes sortes de données à caractère personnel, qu'elles proviennent de leurs salariés, de leurs clients, de leurs adhérents ou du citoyen lambda. A ce titre, ils sont déjà soumis à des règles de transparence contraignantes.

A l'ère d'un monde numérique sans frontières, le volume et la richesse de ces données (santé, finances, Internet, consommation, etc.), comme la diversité de leurs modes d'exploitation, ne cessent d'évoluer. Le public concerné est, lui, de plus en plus sensibilisé. Toutes les entités et leurs correspondants CNIL doivent donc gérer des risques nouveaux.

Pour faire face à ces révolutions et harmoniser les pratiques au sein de l'Union Européenne, un règlement européen fondamental sur la protection des données à caractère personnel a été publié au Journal Officiel le 4 mai dernier. Les obligations des organismes s'en trouveront largement accrues, les droits des personnes élargis et les pouvoirs de sanction de la CNIL renforcés.

Le règlement européen 2016 / 679 du 27 avril 2016 sur la protection des données personnelles sera applicable à partir du 25 mai 2018 dans tous les pays de l'Union européenne. Il confirme la préservation des données personnelles comme un droit fondamental, et confère au citoyen de l'Union Européenne dorénavant une protection particulière.

Les données à caractère personnel : quels changements pour 2018 ?

Les différents enjeux de cette réforme :

- Répondre aux défis de l'évolution technologique
- Renforcer le respect des droits des individus
- Responsabiliser davantage les entreprises

Les principaux changements pour les entreprises :

- Simplification des démarches administratives (avec la CNIL) : fin des déclarations ?
- Obligation de transparence et de preuve renforcée pour les entreprises
- Augmentation des obligations à la charge du responsable des traitements dans les entreprises
- Notification obligatoire des failles et violations des données à caractère personnel
- Augmentation des sanctions (Amende : 4% du CA mondial)
- L'extraterritorialité : c'est l'extension aux entreprises hors UE des données des citoyens de l'UE

Les principaux changements pour les citoyens :

- Droit à l'oubli : droit du citoyen à voir supprimer ses données personnelles
- La portabilité des donnés : la personne peut demander le transfert de ses données
- **Recueil complet du consentement des personnes**
  - ✓ Consentement séparé de tout autre consentement
  - ✓ Consentement spécifique, informé et non-ambigu
  - ✓ Forme claire et intelligible
  - ✓ Pas de consentement implicite
  - ✓ Pas de pré-cochage

- Droit d'accès, de rectification et d'opposition des données
- Droit à la limitation du traitement des données personnelles

Les droits d'information :

- Informer de la **durée de conservation des données**
- Droit de **retirer son consentement** et du droit d'effacement
- Droit d'agir auprès de la CNIL

Des critères qui évoluent également : la collecte des données :

- Une collecte **loyale** et **licite**
- Une collecte réalisée pour **des finalités déterminées**, explicites et légitimes
- Les données doivent être adéquates, pertinentes et non excessives
- Les données doivent être conservées sous une forme permettant l'identification des personnes
- Les données doivent être conservées pendant une durée qui n'excède pas la durée nécessaire aux finalités

Ce qu'il faut retenir :

- **Les droits des individus se renforcent**
- **Augmentation de la responsabilité des entreprises**
- **Simplification des démarches administratives : Fin des déclarations des fichiers à la CNIL ?**
- **Le consentement des individus à laisser leurs données personnelles doit être explicite**
- **Droit pour les individus de voir leurs données personnelles supprimées**