LE RÈGLEMENT GÉNÉRAL EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES
RGPD

DIRECCTE GRAND EST		Septembre 2017

Objectifs et caractéristiques

Ce règlement remplace la directive de 1995 qui a donné lieu à des différences d'interprétation significatives entre les Etats.

Il est d'application directe sur tout le territoire de l'Union Européenne et entrera en vigueur le 25/05/2018.

Toutes les entreprises sont concernées dès lors qu'elles possèdent des fichiers contenant des données à caractère personnel de résidents européens quelle que soit leur nationalité

Il a comme objectifs :

- De renforcer et unifier les droits des résidents européens dont les données personnelles pourraient être traitées
- De responsabiliser les acteurs traitant ces données (responsables des traitements et leurs sous-traitants)
- D'instaurer de nouveaux droits pour les résidents européens :
  Droit à l'oubli – Droit de portabilité (récupération des données)
  Droit d'information (sur la finalité des traitements, sur la violation des données)
  Droit de consentement (accord sur le traitement des données)
- **De prévoir des sanctions allant :**
  de 10 à 20 M€ ou
  de 2 à 4% du chiffre d'affaires annuel mondial

Qu'est-ce qu'une donnée personnelle traitée ?

- toute information se rapportant à une personne physique identifiée ou identifiable (nom, n° d'identification, localisation, IP, adresse, données de santé, revenus, centres d'intérêts etc.)
- Traitements concernés : tous les traitements automatisés ou non (collecte, utilisation, diffusion, effacement etc.)

Qui est concerné ?

- Les responsables du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement : tous les acteurs économiques européens sont concernés dès lors qu'ils traitent des données à caractère personnel
- Leurs sous-traitants : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

Avantages pour l'entreprise

- Instaurer une véritable politique de gestion des traitements des données pour une meilleure connaissance des clients, anticipation et personnalisation de leurs attentes pour une meilleure fidélisation

- Augmentation de la valeur de l'information (et donc de l'entreprise) contenue dans les fichiers ou les bases de données de l'entreprise
  Un traitement non conforme n'est pas commercialisable
- Meilleure image pour l'entreprise : protection des données des clients, responsable, soucieuse de la vie privée et des droits fondamentaux de la personne, bonne réputation, confiance etc.
- Se prémunir contre les contentieux et éviter les sanctions

Trois grandes nouveautés

- Le respect des obligations en matière de données personnelles peut être conjointement partagé entre plusieurs responsables pour un même traitement notamment avec le ou les sous-traitant(s)
- La protection des données se réfléchit dès la conception du traitement (privacy by design/privacy by default)
- Principe de responsabilité (accountability, renversement de la charge de la preuve) : les responsables du traitement doivent démontrer leur conformité (compliance) au règlement

Actions à mener dans l'entreprise

- Désigner un Délégué à la protection des données (DPP ou DPO data protection officer), missions d'information, de conseil et de contrôle en interne
- Cartographier/auditer les traitements actuels et déterminer leurs finalités ainsi que leur durée - Créer un registre des activités de traitement
- Prioriser les actions à mener au regard de la valeur de l'information détenue et des risques sur les droits et libertés des personnes
- Analyser l'impact des traitements sur la protection des données
- Revoir les contrats de sous-traitance informatique et de gestion des données
- Mise en place des mesures techniques et organisationnelles
- Assurer la transparence et l'information des personnes dont les données font ou vont faire l'objet d'un traitement (consentement clairement obtenu) et les informer si incident sur le traitement
- Notifier à la CNIL dans les 72h la survenance d'une faille ou intrusion
- Constituer et regrouper la documentation nécessaire pour démontrer la conformité au règlement
- Possibilité de certifications par un organisme extérieur agréé par la CNIL

Références et contacts

- **Voir le site de la CNIL :**

https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

Contacts

- **Contacts à la DIRECCTE :**

- 67, 68 : vincent.rhin@direccte.gouv.fr, Tél : 03 69 20 99 41
- 08, 10, 51, 52 : richard.dillon@direccte.gouv.fr, Tél :03 26 69 57 49
- 54, 55, 57, 88 : francoise.chauder@direccte.gouv.fr, Tél :03 54 48 20 36

- **Le Délégué régional Grand Est de l'ANSSI :**

- michel.rochelet@ssi.gouv.fr, Tél : 06 45 23 42 75