

# RGPD

## LE RGPD\*, ÇA CHANGE QUOI ?

### Les sanctions sont plus lourdes

Une violation des obligations générales du responsable de traitement pourra coûter 2% du CA annuel mondial d'une entreprise ou 10 millions d'euros (on retient le plus élevé), en cas de non respect d'une injonction, des principes de base d'un traitement, ou des transferts hors UE ou "double la mise" (4% - 20 millions).

### Un règlement applicable à l'UE sans transposition

La déclinaison par chaque Etat Membre n'est plus possible. Certaines dispositions devront cependant être précisées par chacun.

### Un champ territorial étendu

Désormais une société établie en dehors de l'UE pourra être soumise au RGPD dès lors qu'elle offre des services ou des biens à des personnes concernées dans l'UE.

### Il faut notifier les violations de sécurité

Le responsable de traitement devra notifier les violations de sécurité à la CNIL dans les 72h. En cas de risque élevé, il notifie aussi les personnes concernées. Le sous-traitant notifie le responsable de traitement dans les meilleurs délais.

### Davantage de responsabilités pour les sous-traitants

Désormais directement responsables de certaines dispositions, les sous-traitants pourront être sanctionnés par la CNIL et devront tenir un registre.

### Gestion par les risques via les Privacy Impact Assessments (PIA)

Les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés d'une personne devront faire l'objet d'une analyse d'impact. Si l'analyse confirme le risque élevé, la CNIL devra être consultée.

### Plus de données sensibles

La définition des données sensibles est élargie : on ajoute les données génétiques et biométriques. Leur traitement est, en principe, interdit.

### Accountability, LE principe à appliquer

Le régime déclaratif auprès de la CNIL est terminé, désormais les entreprises devront être capables de fournir la documentation, justifier leurs choix, tracer les actions et prouver leur conformité.

### Une ressource clé: le Data Protection Officer

Obligatoire pour les autorités/organismes publics et pour les responsables de traitements réalisés "à grande échelle" et leurs sous-traitants.

### De nouveaux droits

Droit à la portabilité, à l'oubli, protection des mineurs, organiser le sort de ses données après sa mort, droit à la limitation.

\* Le Règlement Général pour la Protection des Données sera applicable à partir du 25 mai 2018.