

THÈME

Synthèse

Les principaux changements issus du RGPD

- « **Accountability** »
 - = responsabilisation de l'employeur comme responsable du traitement : les employeurs devront pouvoir justifier à tout moment de la conformité d'un traitement de données personnelles avec le RGPD
 - ✓ Remplacement du régime déclaratif préalable auprès de la CNIL par l'établissement d'un **registre des activités de traitement** et, en fonction de certains critères, par des **études d'impact** établies par l'employeur
 - ✓ Documentation et mise à jour de la conformité par l'employeur
 - ✓ **Contrôle et sanction à posteriori** par la CNIL : amendes administratives accrues (10 ou 20 millions d'euros, ou de 2% jusqu'à 4% du chiffre d'affaire annuel mondial, le montant le plus élevé étant retenu).
- Renforcement de **l'obligation d'information, de transparence et de loyauté** vis-à-vis des salariés
- Obligation d'**information en cas d'atteinte à la sécurité** des données

Le nouveau pilote de la mise en œuvre de protection des données dans l'entreprise : Délégué à la protection des données (le « DPO »)

- **Désignation obligatoire** uniquement pour les entreprises dont l'activité de base amène (i) à réaliser un suivi régulier et systématique à grande échelle des personnes, ou (ii) à traiter à grande échelle des données dites sensibles.
 - ✓ Dans les autres entreprises, désignation du DPO vivement recommandée par la CNIL
 - ✓ Peut être un salarié de l'entreprise ou désigné en externe
- **Missions :**
 - ✓ Conseiller le responsable du traitement des données
 - ✓ Contrôler le respect du RGPD
 - ✓ Conseiller l'entreprise lors de l'établissement des études d'impact et en vérifier l'exécution
 - ✓ Point de contact de l'autorité de contrôle
 - ✓ Exigence supplémentaire par rapport aux anciens CIL : le DPO doit avoir des connaissances spécialisées du droit et des pratiques en matière de protection des données, et entretenir ses connaissances