

Le règlement général sur la protection des données GDPR



RÉGION ACADÉMIQUE
AUVERGNE-RHÔNE-ALPES

MINISTÈRE
DE L'ÉDUCATION NATIONALE
MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION



Le règlement général sur la protection des données GDPR (général data protection regulation, GDPR) est entré en vigueur le 25 Mai dernier. Ce texte supranational incite les organisations et les entreprises à être davantage vigilantes concernant l'exploitation des données personnelles. Il viendra remplacer la loi informatique et libertés de 1978 en France.

Qui est concerné ? Tous les organismes publics et privés qui traitent, manipulent, gèrent ou stockent des données à caractère personnel et notamment dans l'Union européenne. Un comité de protection des données va surveiller et garantir la mise en œuvre de ce règlement au niveau européen.

Pourquoi le GDPR ? Il s'agit de protéger les individus contre une utilisation malveillante ou abusive de leurs données personnelles. Il s'agit également d'uniformiser des pratiques au niveau international et ceci notamment au sein de l'Union européenne. Il s'agit, enfin, de responsabiliser les entreprises sur la collecte, l'utilisation et la sauvegarde des données personnelles.

Quelles conséquences ?

➤ **pour les entreprises ?** Elles vont devoir :

- **Evaluer** l'outillage de sécurité des systèmes d'information et les dispositifs de sécurité existants puis identifier les écarts et les faiblesses pour mettre en place une feuille de route de mise en conformité.
- **Notifier** à la Cnim les incidents de sécurité dans les 72 heures qui suivent la découverte d'une violation de données à caractère personnel.
- **Nommer** un délégué à la protection des données pour les entreprises du secteur public et dans les entreprises dont l'activité principale amène à des traitements à grande échelle de données sensibles comme les données religieuses, judiciaires, etc. ou relative à des condamnations pénales et certaines infraction

➤ **Pour les particuliers ?** Ils vont bénéficier de plusieurs protections :

- **Droit à l'oubli pour les mineurs** : lorsqu'une personne était mineure au moment de la collecte des données, elle peut exiger leur effacement. Pour les mineurs de moins de 16 ans, le consentement d'un parent ou responsable légal est obligatoire et les entreprises doivent adapter leurs contenus pour que ceux-ci leur soient intelligibles.
- **Demande de modification par voie électronique** : le nouveau règlement permet aux utilisateurs l'accès, la rectification ou l'opposition aux données par voie électronique
- **Limitation de la conservation des données** : La durée de conservation des données doit être définie et varie en fonction de la nature et de la finalité (Ex : données relatives au paiement : uniquement le temps de la transaction). Ensuite, elles doivent être effacées
- **Transfert des données** : un utilisateur peut récupérer et transmettre toutes les données collectées d'une plateforme vers un autre réseau de son choix (Ex : réseau social, fournisseur d'accès etc.)
- **Le contact unique** : en cas de problème, l'utilisateur ne se retourne plus vers l'entreprise qui possède ses données mais vers l'autorité de protection des données

Quelles sont les sanctions possibles ? Des amendes et pénalités sur le chiffre d'affaire mondial réalisée par l'entreprise défaillante seront prises à son encontre en cas de non- respect de cette nouvelle réglementation.

