

RGPD : Ce qu'il faut savoir pour le diplôme RNCP Niveau 7

Qu'est-ce que le RGPD ?

Le Règlement Général sur la Protection des Données (RGPD) est une loi européenne entrée en vigueur en mai 2018. Elle vise à protéger les données personnelles des citoyens européens et impose des règles aux entreprises qui les collectent et les traitent.

Objectifs principaux du RGPD

1. Protéger les données personnelles des citoyens européens.
2. Responsabiliser les entreprises qui collectent et utilisent ces données.
3. Donner plus de contrôle aux utilisateurs sur leurs informations.
4. Harmoniser les règles au sein de l'Union Européenne.

Principes fondamentaux du RGPD

1. Licéité, loyauté et transparence : Informer clairement l'utilisateur sur l'utilisation de ses données.
2. Limitation des finalités : Collecter des données uniquement pour un objectif précis.
3. Minimisation des données : Ne collecter que les données strictement nécessaires.
4. Exactitude des données : Maintenir des données à jour et exactes.
5. Limitation de conservation : Ne pas stocker les données plus longtemps que nécessaire.
6. Intégrité et confidentialité : Sécuriser les données contre tout accès non autorisé.

Droits des utilisateurs

1. Droit d'accès : Toute personne peut demander quelles données sont collectées sur elle.
2. Droit de rectification : Modifier des données incorrectes ou incomplètes.
3. Droit à l'effacement ('droit à l'oubli') : Demander la suppression de ses données.
4. Droit à la portabilité : Récupérer ses données et les transférer vers un autre service.
5. Droit d'opposition : Refuser l'utilisation de ses données.
6. Droit de limitation du traitement : Restreindre temporairement l'utilisation de ses données.

Obligations des entreprises

1. Obtenir un consentement clair et explicite pour collecter des données.
2. Tenir un registre des traitements de données.
3. Nommer un DPO (Délégué à la Protection des Données) si nécessaire.
4. Assurer la sécurité des données (chiffrement, accès restreint, etc.).
5. Notifier toute violation de données dans un délai de 72 heures à la CNIL (ou autre autorité compétente).

Sanctions en cas de non-respect

- Amende pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial.
- Suspension des activités liées aux données personnelles.
- Perte de confiance des utilisateurs.

Cas concrets et exemples

- Google a été condamné à 50 millions d'euros d'amende pour non-respect du RGPD en 2019.
- Facebook et Amazon ont aussi été sanctionnés pour gestion opaque des données.
- Une entreprise qui envoie des newsletters sans consentement peut être pénalisée.

Ce qu'un Data Analyst doit retenir

- S'assurer que les données collectées sont justifiées et nécessaires.
- Anonymiser les données quand c'est possible.
- Ne pas partager des données sans autorisation.
- Respecter les droits des utilisateurs et faciliter leur exercice.
- Collaborer avec le DPO pour garantir la conformité.