

1. Définition du règlement général de protection des données (RGPD)



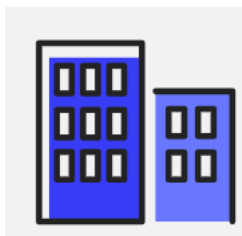
Le RGPD est un texte de référence européen qui règlemente pour toute entreprise/organisme la gestion des données personnelles de leurs clients/usagers, s'ils sont citoyens européens **ou résidents sur le territoire européen**.

Donnée personnelle : toute information se rapportant à une personne physique identifiée ou identifiable (nom, adresse, email, numéro de téléphone, adresse IP, identifiant de connexion, etc.)

Donnée sensible : catégorie particulière de données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, l'appartenance syndicale, les données de santé, la vie sexuelle, les données biométriques ou génétiques.

Ce règlement porte sur la collecte, la conservation et le traitement des données, avec des conditions **beaucoup plus restrictives** pour les organismes s'il s'agit de données sensibles.

Extraits du RGPD , principes fondamentaux



a) Principe de minimisation et de finalité

- La collecte de données doit servir un **objectif déterminé, explicite et légitime**
- Ne collecter **que les données strictement nécessaires** à cette finalité
- Les données ne peuvent pas être réutilisées pour un autre objectif sans nouveau consentement

b) Principe de transparence et d'information

- Les personnes doivent être **clairement et simplement informées** de l'utilisation qui sera faite de leurs données **avant** la collecte
- Cette information doit préciser : qui collecte, pourquoi, combien de temps les données seront conservées, qui y aura accès
- Le traitement n'est pas forcément informatisé : tout traitement de données (même papier) rentre dans le cadre du RGPD

c) Principe de consentement L'organisme doit recueillir un **consentement valide** de la part de la personne. Pour être valide, le consentement doit être :

- **Libre** : la personne doit avoir un véritable choix, sans contrainte ni conséquence négative en cas de refus
- **Spécifique** : un consentement par finalité (on ne peut pas demander un consentement global pour plusieurs usages différents)
- **Éclairé** : la personne doit comprendre à quoi elle consent
- **Univoque** : par un acte positif clair (cocher une case, cliquer sur un bouton). Les cases pré-cochées sont interdites

Attention : Pour les **données sensibles**, le consentement doit être **explicite** (déclaration écrite ou confirmation électronique claire).

d) Principe de limitation de la conservation

- Les données ne peuvent être conservées que **le temps nécessaire** à la finalité prévue
- Passé ce délai, elles doivent être supprimées ou anonymisées

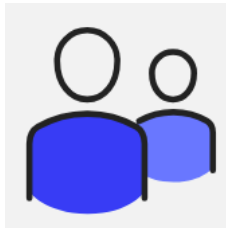
e) Obligation de sécurité

- L'organisme qui réalise la collecte doit **sécuriser ces données** (mesures techniques et organisationnelles)
- Il doit **notifier la CNIL sous 72h** en cas de violation de données (piratage, perte, accès non autorisé)
- Si le risque est élevé pour les personnes, l'organisme doit **aussi informer les personnes concernées**

f) Responsabilité de l'organisme

- L'organisme doit être en mesure de **prouver** qu'il respecte le RGPD (principe d'accountability)
- Il doit permettre aux personnes d'**exercer facilement leurs droits**

2. Droit des personnes



Le but est de rendre la maîtrise de leurs données personnelles (DP) aux citoyens européens. Ceux-ci ont le droit de :

- **Droit d'accès** : savoir si des données les concernant sont traitées et lesquelles
- **Droit de rectification** : corriger des données inexactes
- **Droit à l'effacement** ("droit à l'oubli") : demander la suppression de leurs données dans certains cas (consentement retiré, données non nécessaires, opposition au traitement)
- **Droit à la portabilité** : récupérer leurs données sous un format lisible par une machine (pour les réutiliser ou les transmettre à une entreprise concurrente)
- **Droit d'opposition** : refuser un traitement de données (notamment pour la prospection commerciale)
- **Droit à la limitation** : demander le gel temporaire du traitement dans certaines situations

Conditions d'exercice pour les personnes:

- Être informé de la finalité, de la durée de conservation, des destinataires
- Pouvoir retirer son consentement **aussi facilement qu'il a été donné**
- Être informé par l'organisme de la démarche à suivre en cas de litige (la CNIL en France)

3. La commission nationale pour l'informatique et liberté (CNIL)



Cet organisme public a pour mission de faire appliquer le RGPD en France.

Rôles de la CNIL :

- Informer et conseiller les citoyens et les organismes
 - Contrôler le respect du RGPD et sanctionner les manquements: amendes jusqu'à 20 millions d'euros OU 4% du chiffre d'affaires annuel mondial de l'entreprise (**le montant le plus élevé des deux**).
 - Accompagner la conformité des entreprises
- Traiter les réclamations des citoyens
- Le but de cette commission est de veiller au bon usage et à la protection des données personnelles, et de faire en sorte que leur utilisation ne porte pas atteinte aux libertés individuelles.

Travail à l'oral (5 min, devant la classe)

Votre professeur va vous attribuer un sujet parmi les 12 sujets ci-dessous. Vous travaillerez en groupe de 2 ou 3 élèves. Pour préparer votre réponse :

- Répondre à la question de manière argumentée, en utilisant et en citant des éléments du cours sur le RGPD.
- trouver un cas réel médiatisé en lien avec leur question (exemples : sanction de Google, Facebook, plainte contre un réseau social, etc.)
- Créer une affiche de sensibilisation sur le sujet (format A4, à utiliser avec la caméra de projection)

Question 1 : Lorsque vous acceptez la collecte, transfert, sauvegarde, et l'utilisation de vos données par un professionnel : Doit-il vous informer de l'utilisation qui est faite de vos données pour différents usages?

Ou bien fait-il ce qu'il veut ? Après tout, vous avez bien coché la case ... 

Question 2 : Les entreprises américaines comme Uber ou Amazon, ..., doivent-elles se conformer au RGPD?



Question 3 : Un site marchand européen a-t-il le droit de garder mes coordonnées bancaires indéfiniment pour faciliter mes futurs achats ?



Question 4 : Je n'utilise plus mon compte sur un réseau social **et je ne le supprime pas**. Mes données sont-elles conservées ? Ai-je un recours ?



Question 5 : Peut-on m'imposer de recevoir des publicités pour valider ma participation à un jeu concours ?



Question 6 : Le site Internet du restaurant-livreur de pizza, sur lequel vous avez renseigné des données personnelles est victime de hacking. Est-ce grave ? Doit-il informer ses clients ? Est-il responsable de l'usage qui sera fait de ces données ?



Question 7 : J'ai accepté qu'une application de sport collecte mes données (rythme cardiaque, poids, sommeil) pour suivre mes entraînements. A-t-elle le droit de les transmettre à une compagnie d'assurance ? Et si je change d'avis, puis-je retirer mon consentement ?



Question 8 : Une entreprise française a-t-elle le droit de stocker les données de ses clients sur des serveurs situés hors de l'Union européenne (aux États-Unis, en Inde...) ?



Question 9 : J'ai postulé pour un job d'été et ma candidature n'a pas été retenue. L'entreprise peut-elle garder mon CV aussi longtemps qu'elle le souhaite ?



Question 10 : Je voudrais savoir quelles informations un réseau social possède sur moi, et les récupérer pour les transférer sur une autre plateforme. En ai-je le droit ? Comment faire ?



Question 11 : Un site Internet peut-il m'empêcher de consulter ses articles si je refuse les cookies publicitaires ?



Question 12 : Une employée d'une clinique envoie par erreur un fichier contenant les noms et dossiers médicaux de patients à une mauvaise adresse e-mail. S'agit-il d'une violation de données, même sans piratage ? Que doit faire la clinique ?

