

- Le Règlement Général sur la Protection des données (RGPD) concerne tout individu à chaque moment de sa vie : de la maternité à l'université, en passant par ses déplacements, les soins médicaux, ses activités professionnelles, etc.
- L'objectif du RGPD est donc de protéger ces données personnelles ou encore de proposer un cadre de protection des données à l'échelle de l'UE. Il garantit une sécurité optimale des informations traités et permet aux personnes de mieux comprendre et de mieux contrôler l'utilisation de leurs données.
- Le respect du RGPD se fait par trois organismes :

Organisme	Echelle	Missions
Commission Nationale de l'Informatique et des libertés (CNIL)	Nationale	<ul style="list-style-type: none"> - Informer, protéger les droits - Accompagner, conseiller - Anticiper, innover - Contrôler, sanctionner
Comité Européen de la protection des Données (CEPD)	Européenne	<ul style="list-style-type: none"> - Coordonne l'action des CNIL de l'UE - Conseille la commission européenne sur des questions du RGPD - Garantit la bonne application du RGPD - Donne son avis sur les projets de décisions des autorités de contrôle de chaque pays européen
Cour de Justice de l'Union Européenne (CJUE)	Européenne	<ul style="list-style-type: none"> - Veille à l'application de la législation de l'UE - Sanctionne

- Les différents types de donnée à caractère personnel :

Type de donnée ...	Exemple
... directement identifiante	Nom, prénom, mail, photo
... indirectement identifiante	N° de sécurité sociale, empreinte digitale, pseudo, matricule interne, n° client
Toute combinaison d'informations permettant d'identifier la personne	Date de naissance, lieu de résidence, nom de l'employeur, lieu de naissance, sexe, loisir

- 5 recommandations sur les règles de gestion à mettre en place pour respecter les normes RGPD :
 - Sélectionner uniquement les données nécessaires
 - Droits des personnes : accès, suppression, modification
 - Les personnes doivent être informés de l'utilisation des données les concernant et de la manière dont ils peuvent exercer leurs droits
 - Prévenir les risques d'atteinte à la sécurité des données, assurer la sécurité des données traitées
 - Désigner un DPO (*Data Protection Officer*) pour piloter la gouvernance des données et protéger les droits fondamentaux des personnes concernées

Source :

https://sante.gouv.fr/IMG/pdf/memento_rgpd-a5-190401-vf.pdf

<https://www.cnil.fr/fr/comprendre-le-rgpd/le-mooc-de-la-cnil-est-de-retour-dans-une-nouvelle-version-enrichie>

<https://www.cnil.fr/fr/comprendre-le-rgpd/les-six-grands-principes-du-rgpd>

- 5 recommandations sur les règles de gestion à mettre en place sur les données du CRM :
 - Sélectionner uniquement les données nécessaires :
 - Enlever : groupe sanguin, numéro sécurité sociale, id site web
 - Garder uniquement id du client
 - Droits des clients : accès, suppression, modification
 - Les personnes doivent être informés de l'utilisation des données les concernant et de la manière dont ils peuvent exercer leurs droits
 - Prévenir les risques d'atteinte à la sécurité des données, assurer la sécurité des données traitées
 - Fixer une limite de conservation des données : 2 ans après la fin de leur contrat

Source :

<https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees-du-secteur-de-lassurance>

<https://entreprendre.service-public.fr/vosdroits/F24270>