

Règlement Général sur la Protection des Données (RGPD)

DRAME Ibrahima
KOURBANHOUSSEN Idriss

Problématique

Comment les entreprises peuvent-elles s'adapter au Règlement Général sur la Protection des Données (RGPD) afin d'assurer la protection et le respect des données personnelles, tout en optimisant leurs opérations ?

Sommaire

- I. Contexte et objectifs du RGPD**
- II. Champ d'application et principes fondamentaux**
 - A. Champ d'application du RGPD
 - B. Principes fondamentaux du RGPD
- III. Droits des individus**
- IV. RGPD pour les entreprises**
 - A. Responsabilités des entreprises
 - B. Sanctions pour les entreprises
- V. Schéma global du RGPD**
- VI. Rapprochement avec d'autres aspects du cours**
 - A. Access lists
 - B. Network forensics
- VII. Conclusion**
- VIII. Références**





I. Contexte et objectif du RGPD

- En janvier 2012, la Commission européenne propose une réforme des règles de protection des données.
- Adopté par le Parlement européen en mars 2014, le règlement entre en vigueur le **25 mai 2018**, devenant obligatoire pour tous les États membres de l'UE à partir de cette date.
- **Objectif** : Redonner le contrôle des données aux citoyens et simplifier la réglementation pour les entreprises. Renforcer la protection de la vie privée des citoyens et instaurer des règles claires sur la collecte, le stockage, le traitement et la transmission des données personnelles.
- **Scandale Facebook-Cambridge Analytica** : Vol et manipulation de données personnelles à des fins électorales, qui a éclaté peu de temps avant l'entrée en vigueur du règlement, souligne l'importance de ces nouvelles règles.

II. Champ d'application et principe fondamentaux

A. Champ d'application du RGPD

- Le RGPD établit un cadre complet pour le traitement des données personnelles en Europe, axé sur la protection des droits fondamentaux et de la vie privée.
- ***“Le RGPD s'applique à une vaste gamme de données personnelles, définies comme toute information permettant d'identifier directement ou indirectement une personne physique.”***
- Cela englobe des données aussi diverses que les noms, les adresses, les numéros d'identification, les données de localisation, les adresses IP, les cookies, et d'autres informations qui sont spécifiques à l'identité d'une personne.



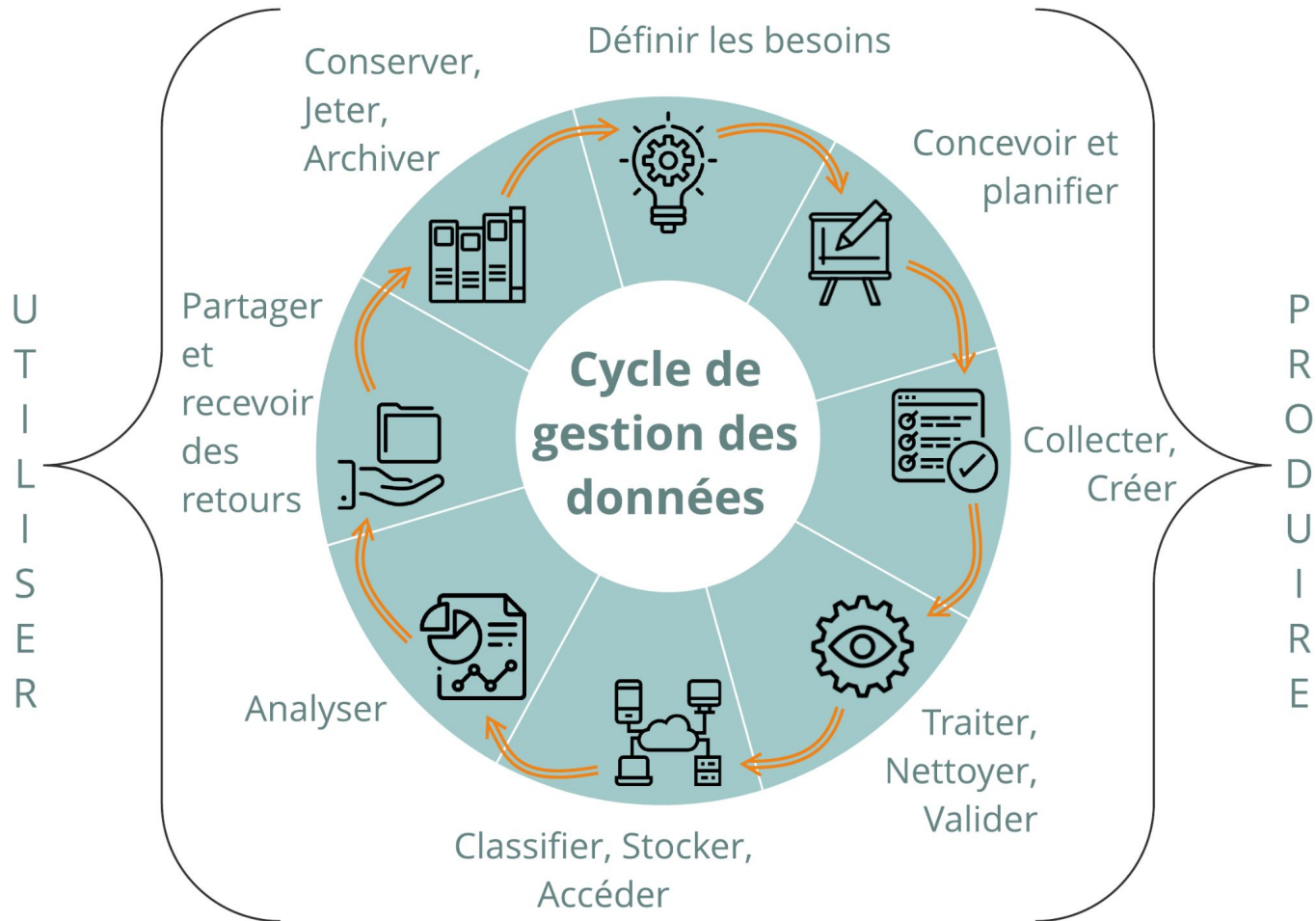


Qu'est-ce qu'une donnée personnelle ?

Toute information relative à un particulier identifié ou identifiable, directement ou indirectement, grâce à un identifiant ou à un ou plusieurs éléments propres à son identité

Par exemple :





II. Champ d'application et principe fondamentaux

B. Principe fondamentaux du RGPD

- **Légitimité, loyauté et transparence** : Traitement des données de manière licite, équitable et transparente en informant les individus sur la manière dont leurs données seront utilisées.
- **Finalité limitée** : Collectes à des fins spécifiques, explicites et légitimes, et ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités initiales.
- **Minimisation des données** : Seules les données nécessaires à la réalisation des objectifs préétablis doivent être collectées.
- **Exactitude** : Prises de mesure pour garantir que les données inexactes soient corrigées ou effacées.
- **Limitation de la conservation** : Les données personnelles ne doivent être conservées que le temps nécessaire pour atteindre la finalité pour laquelle elles ont été collectées.



III. Droits des Individus



- **Le droit à l'information** : Information claire et compréhensible sur la collecte et le traitement des données telles que la finalité du traitement, les destinataires des données, la durée de conservation, et les droits des individus.
- **Le droit d'accès** : Pouvoir de vérifier si leurs données personnelles sont traitées, et dans l'affirmative, d'obtenir des informations détaillées sur ce traitement. Accès gratuit à une copie des données personnelles traitées, et ce, dans un délai d'un mois à compter de la demande.
- **Le droit de rectification** : Possibilité de corriger toute inexactitude dans leurs données personnelles.
- **Droit d'effacement** : Souvent appelé le "droit à l'oubli", permet la demande de suppression de leurs données lorsque celles-ci ne sont plus nécessaires aux fins initiales du traitement.
- **Le droit à la portabilité** : Demander la transmission directe de leurs données à un autre responsable du traitement, facilitant ainsi la mobilité des informations personnelles d'un service à un autre.
- **Le droit d'opposition** : permet aux individus de s'opposer au traitement de leurs données personnelles dans certaines circonstances.

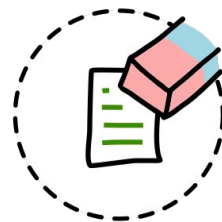
RGPD : les droits de la personne



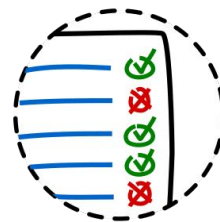
Accès



Rectification



Effacement



Limitation



Opposition



Portabilité



Réclamation



Actions

IV. RGPD pour les Entreprises

A. Responsabilités des Entreprises



- **Responsable de Traitement (Entreprise) :**
 - Identifier et définir les finalités du traitement des données personnelles.
 - Assurer que le traitement est conforme aux principes fondamentaux du RGPD.
 - Mettre en place des mesures de sécurité appropriées pour protéger les données.
 - Être transparent avec les individus concernant le traitement de leurs données.
- **Sous-traitant :**
 - Traiter les données personnelles uniquement selon les instructions du responsable de traitement.
 - Mettre en place des mesures de sécurité adéquates pour protéger les données traitées.
 - Informer immédiatement le responsable de traitement en cas de violation de données.
- **Délégué à la Protection des Données (DPO) :**
 - Surveiller la conformité au RGPD au sein de l'entreprise.
 - Conseiller l'entreprise sur les obligations en matière de protection des données.
 - Coopérer avec l'autorité de contrôle et servir de point de contact pour les questions relatives à la protection des données.
- **Autorité de Contrôle :**
 - Superviser et garantir le respect du RGPD sur le territoire.
 - Recevoir les notifications de violations de données et prendre des mesures appropriées.
 - Fournir des conseils et des orientations aux entreprises et aux individus.

6 ÉTAPES POUR VOUS PRÉPARER AU RGPD

Désigner un Délégué à la Protection des Données (DPO)

Intégrer le RGPD aux process de votre entité et assurer sa mise en œuvre.



Cartographier les traitements de données à caractère personnel

Répertorier les données traitées et leur stockage (lieu, temps, règle de transmission).



Prioriser les actions à mener

Identifier les traitements de données à risques et prendre des mesures pour protéger les personnes concernées.



Gérer les risques

Mettre en place des actions pour diminuer les risques qui pèsent sur la vie privée des personnes concernées par vos traitements.



Documenter la conformité

Créer un dossier regroupant les documents qui démontrent le bon respect du RGPD.

Organiser les processus internes

En cas d'incident, vos services doivent savoir à qui s'adresser et quoi faire.



IV. RGPD pour les Entreprises

B. Sanctions pour les Entreprises



- **Amendes financières** : Le RGPD autorise des amendes substantielles pouvant atteindre 4 % du chiffre d'affaires mondial annuel ou 20 millions d'euros, selon le montant le plus élevé.
- **Avertissements et réprimandes** : Les autorités de contrôle peuvent émettre des avertissements officiels ou des réprimandes formelles aux entreprises en cas de violations graves du RGPD.
- **Restrictions sur le traitement des données** : Les autorités de contrôle ont le pouvoir d'imposer des restrictions sur le traitement des données par une entreprise en cas de non-conformité avec le RGPD.
- **Obligation de rectification ou d'effacement des données** : Les autorités de contrôle peuvent obliger une entreprise à rectifier ou à effacer des données personnelles en cas de non-respect des principes du RGPD.
- **Suspendre les transferts de données vers des pays tiers** : En cas de non-conformité, les autorités de contrôle peuvent suspendre ou interdire le transfert de données personnelles vers des pays situés en dehors de l'Espace économique européen.
- **Responsabilité civile** : Outre les sanctions administratives, une entreprise peut être sujette à des actions en responsabilité civile de la part des personnes affectées par la violation.
- **Réparation des préjudices** : Les entreprises peuvent être tenues de réparer les préjudices causés aux personnes concernées par une violation du RGPD.

Les sanctions de la CNIL en 2022

 **21 sanctions** pour un montant de **101 277 900 €**



Un tiers des sanctions comporte un manquement à la **sécurité des données personnelles**



3 décisions de la CNIL en coopération avec d'autres **autorités européennes**

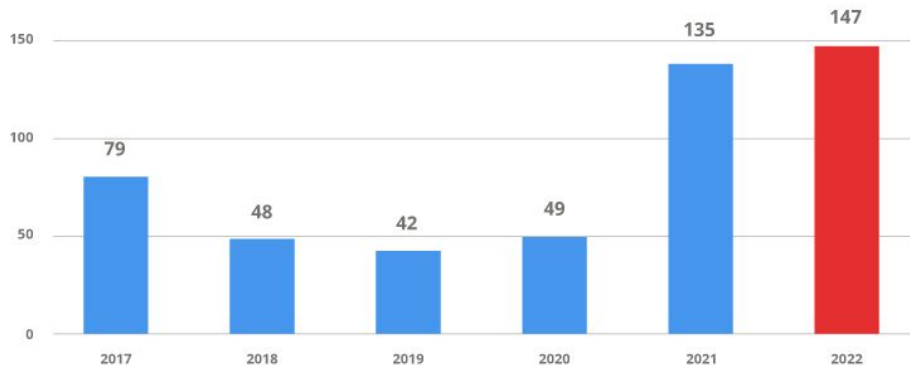
18 dossiers européens examinés par la CNIL



500 millions d'euros d'amendes

prononcées pour des manquements au RGPD, à la loi Informatique et Liberté ou à la directive ePrivacy.

Mises en demeure de la CNIL 2022



Parmi ces sanctions

Amazon

35 M€ en 2020

Microsoft

60 M€ en 2022

Google

50 M€ en 2019
100 M€ en 2020
150 M€ en 2021

Facebook

60 M€ en 2021

Apple

8 M€ en 2022

Autorités européennes de protection des données

2,5 milliards d'euros d'amendes

prononcées par les autorités européennes de protection des données pour des manquements au RGPD

V. Schéma global du RGPD



VI. Rapprochement avec d'autres aspects du cours

A. Access lists

- Access lists:

- Pour déterminer **qui a le droit d'accéder** à des fichiers, des bases de données ou d'autres ressources contenant des données sensibles.
- Permettent de définir les **autorisations d'accès** en fonction des rôles, des responsabilités et des besoins opérationnels, contribuant ainsi à respecter ce principe.
- Enregistrer les accès aux données, assurant ainsi une **traçabilité des activités** d'accès et une identification des utilisateurs responsables.
- En contrôlant l'accès aux données, contribuent à **prévenir** les violations en restreignant l'accès non autorisé.



VI. Rapprochement avec d'autres aspects du cours

B. Network forensics

- **Network forensics:**
 - Les investigations de network forensics sont essentielles pour comprendre **l'origine et l'étendue des incidents** de sécurité, ce qui contribue à l'application des mesures correctives exigées par le RGPD.
 - Permettent de **surveiller les flux de données** en temps réel, assurant ainsi la **protection** des données personnelles lors de leur transmission, conforme aux exigences du RGPD.
 - Aident à **identifier les menaces potentielles** et les comportements malveillants, renforçant la prévention des violations de données et la protection des droits des individus conformément au RGPD.
 - Les données recueillies par les investigations de network forensics peuvent servir de **preuves tangibles en cas d'audit** par les autorités de contrôle du RGPD, démontrant les efforts déployés pour assurer la sécurité des données personnelles.



VII. Conclusion



- Dans un contexte d'évolutions technologiques rapides, le respect de la vie privée demeure essentiel, et le RGPD joue un rôle clé en équilibrant l'innovation technologique avec la protection des droits individuels.
- Les entreprises peuvent s'adapter au RGPD en intégrant des pratiques de gestion des données axées sur la transparence, la sécurité et le respect des droits individuels, tout en exploitant ces efforts pour optimiser leurs opérations et renforcer la confiance de leurs clients.
- Une adaptation continue du RGPD s'avère cruciale dans notre monde ultra-connecté, incitant à une harmonisation entre la protection des données personnelles et les réalités technologiques émergentes, afin d'assurer une coexistence éthique et sécurisée dans notre environnement numérique en constante évolution

VIII. Références



- <https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on>
- https://fr.wikipedia.org/wiki/R%C3%A8glement_g%C3%A9n%C3%A9ral_sur_la_protection_des_donn%C3%A9es
- Cours de “Droit de l'informatique et propriété industrielle” M1 RSA
- Cours de “Sécurité des réseaux et des systèmes autonomes” M2 RSA
- <https://www.economie.gouv.fr/entreprises/reglement-general-protection-donnees-rgpd>
- <https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679>
- <https://www.vie-publique.fr/eclairage/19588-rgpd-reglement-general-sur-la-protection-des-donnees-de-quoi-sagit-il>