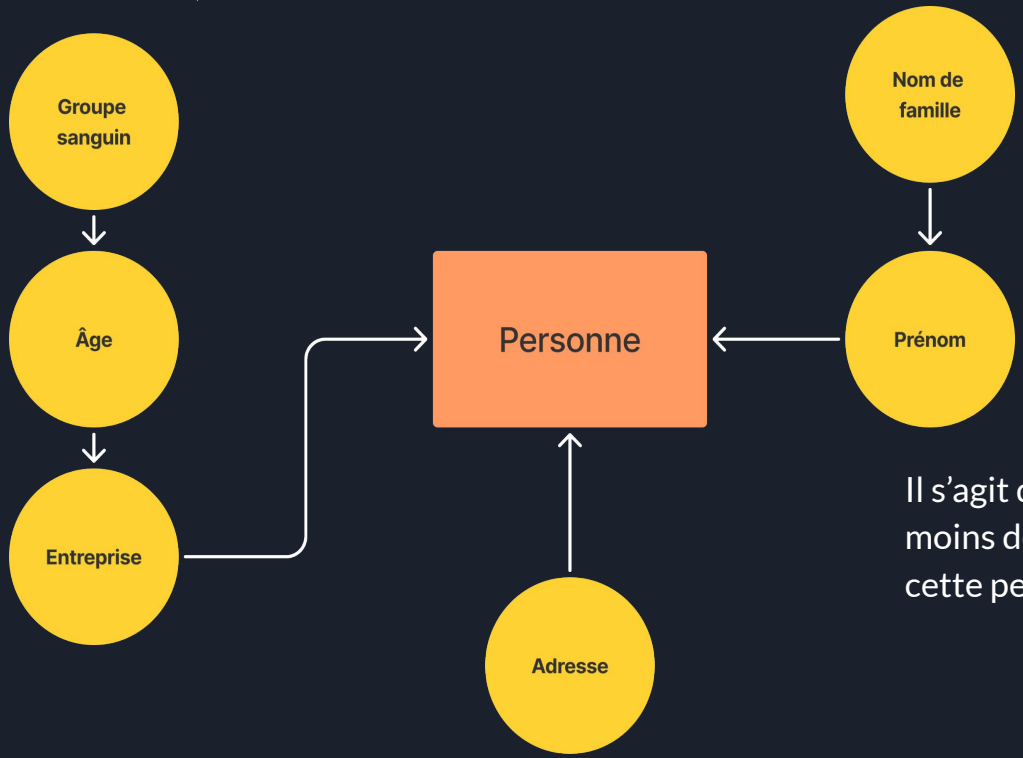
CNIL, RGPD et vous

Présenté par Molinié Thibaut

Quelques définitions

Données personnelles



Éléments qui, pris séparément ou cumulés, permettent d'identifier une personne (un code postal seul n'est pas une donnée personnelle alors qu'une adresse complète, si).

Il s'agit de pouvoir identifier une personne en particulier ou du moins de permettre de réduire les indices jusqu'à détecter cette personne là qui fait qu'il s'agit de données personnelles.

Flux de données

- Flux de données principal :
  - Utilisation quotidienne des données pour le bon fonctionnement de l’application.
- Flux de données secondaire :
  - Support.
  - Actions administrateur.
  - Archivage.

Le RGP... quoi?

Le règlement général de protection des données (RGPD) est un texte réglementaire européen qui encadre le traitement des données.

Son but :

- Encadre :
  - Le traitement.
  - Le stockage.
  - Le consentement des individus.
  - Les sanctions.
- But :
  - Créer un cadre légal.
  - Protéger les individus.

La CNIL c’est quoi ?

Son rôle :

- **Protection des données personnelles** :
  - Informatiques ou papier.
  - Publics ou privés.
- Protéger les individus.
- Alerter.
- Conseiller.
- Informer.
- Contrôler.
- Sanctionner.

Son statut :

- Autorité administrative indépendante (AAI).
- Composée de 18 membres élus ou nommés.

Missions de la CNIL

Identifier

- Une donnée personnelle.
- Sa durée de conservation
- Méthodes de traitement.
- Les actions en cas de fuite.
- Ceux ne respectant pas le RGPD.

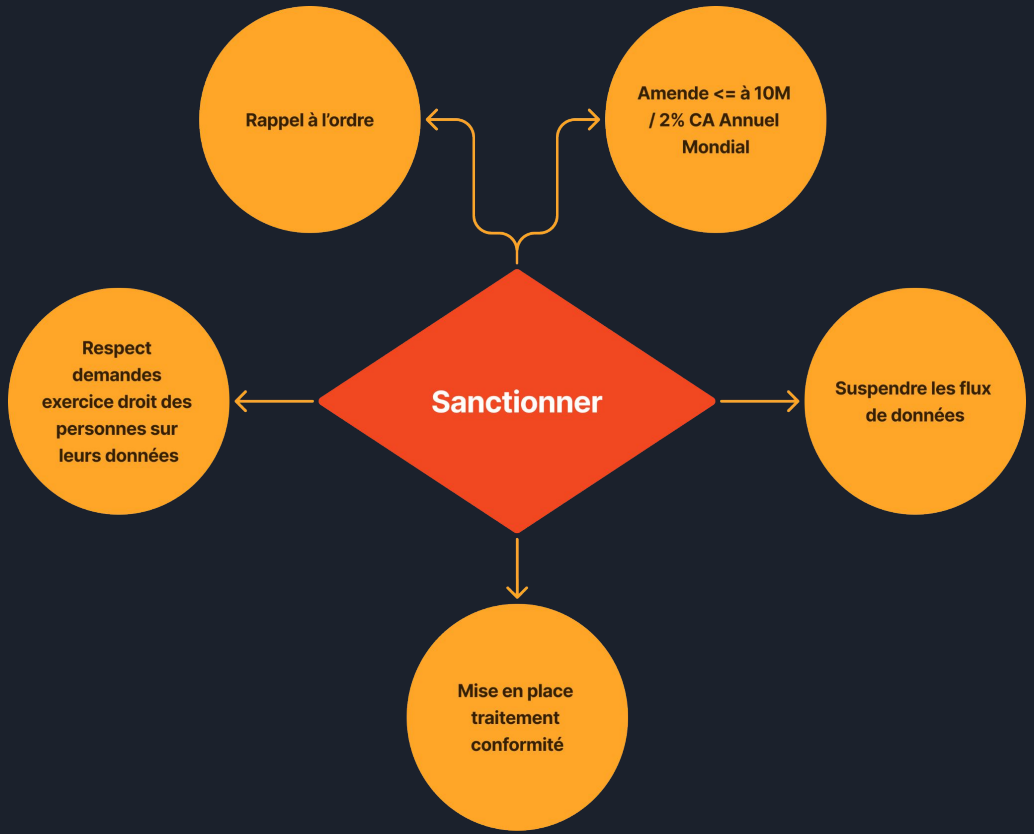
Protéger

- Les individus personne physique ou morale.
- Contre les attaques externes et internes.

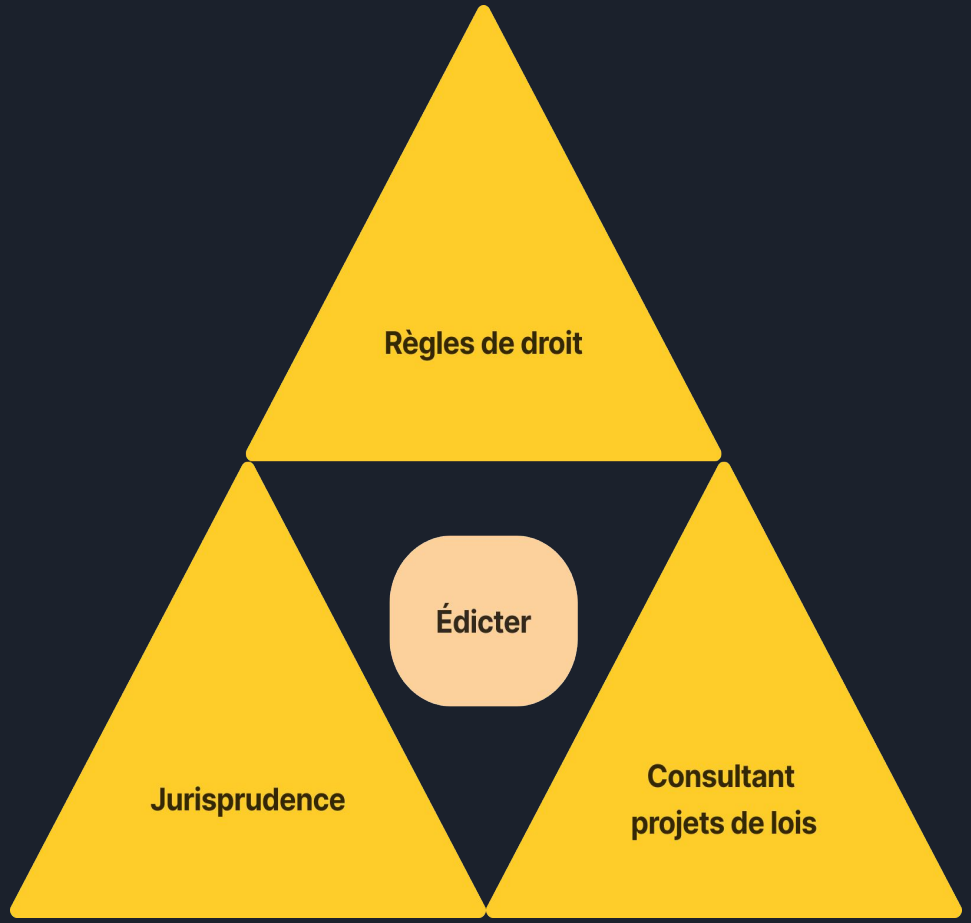
Accompagner

- Appui juridique et technique.
- Revue de conformité.
- Sensibilisation à la protection des données.

Missions de la CNIL



Missions de la CNIL

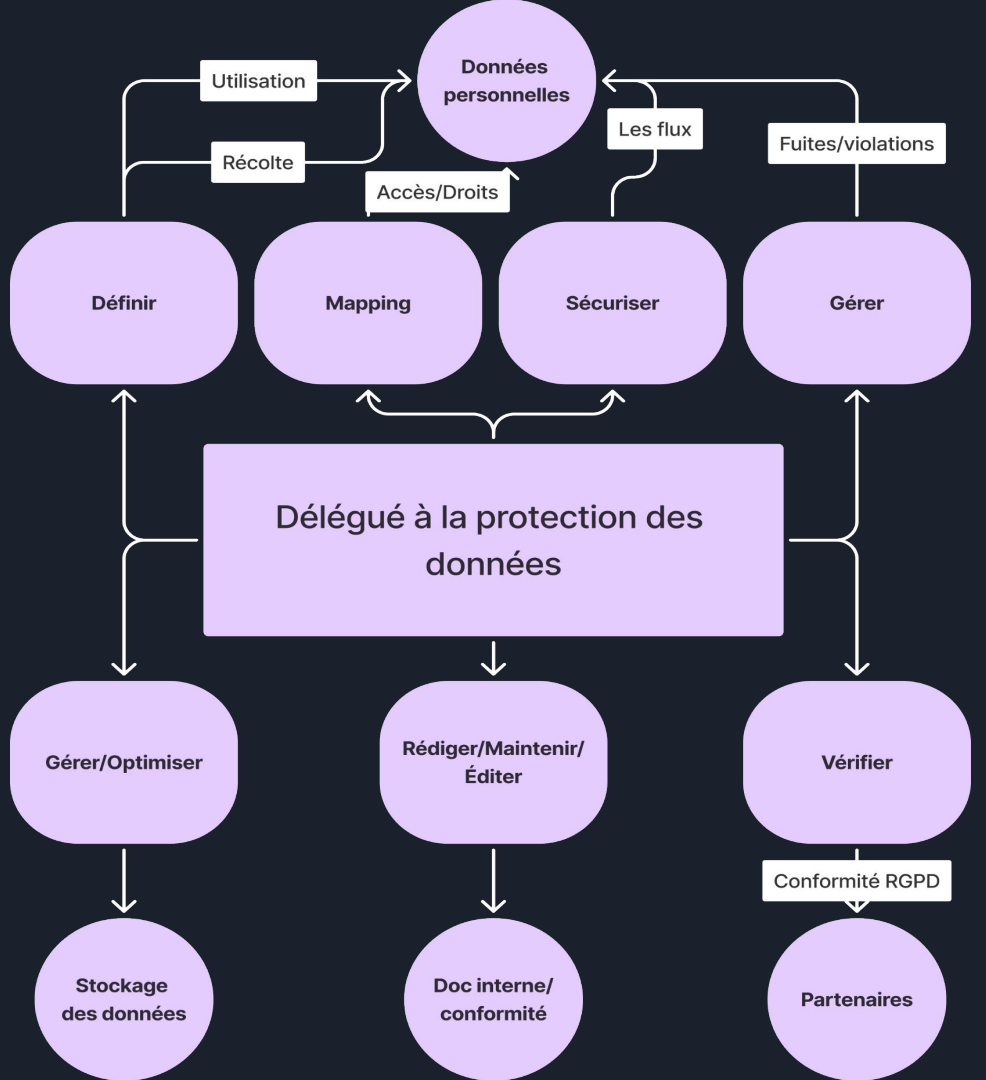


Le rôle Data Protection Officer

Data Protection Officer, ou Délégué à la Protection des Données.

Son rôle est de veiller à ce que le risque de ré-identification avec des moyens raisonnables soit nul.

Mais pas que!



Que faire en cas de divulgation de données personnelles non-anonymisées ?

- Respirer calmement.
- Empêcher toute nouvelle fuite.
- Identifier les utilisateurs touchés.
- Prévenir ces utilisateurs :
  - Informer leurs banques.
  - Modifier leurs identifiants et mots de passe.
  - Rester en contact avec vous.
- Prendre toutes les mesures pour faire retirer ces informations.
- Prévenir la CNIL et demander un accompagnement.
- Renforcement de la sécurité et de communication.

Anonymisation

Action visant à rendre inexploitable des données pour l'identification d'un individu.

L'anonymisation n'est pas équivalente à la pseudonymisation qui permet un retour arrière et donc de retrouver les données initiales avec l'aide de données tierces.

Il existe plusieurs façon d'anonymiser une donnée :

- **La généralisation**.
- **La substitution**.
- **La randomisation**.
- **La permutation**.

Vérifier l’efficacité de l’anonymisation

Prendre un jeu de données anonymisées et tester ces 3 méthodes :

- **L’individualisation**.
- La **corrélation.**
- L’**inférence**.

Et maintenant, un petit test

Contexte :

- Vous êtes développeur back-end.
- On vous confie le développement de l’anonymisation des données en base de données.

Exercice pratique

C’est bien mais on commence par quoi?

- Un cahier des charges.
- La répartition des tâches en équipe.

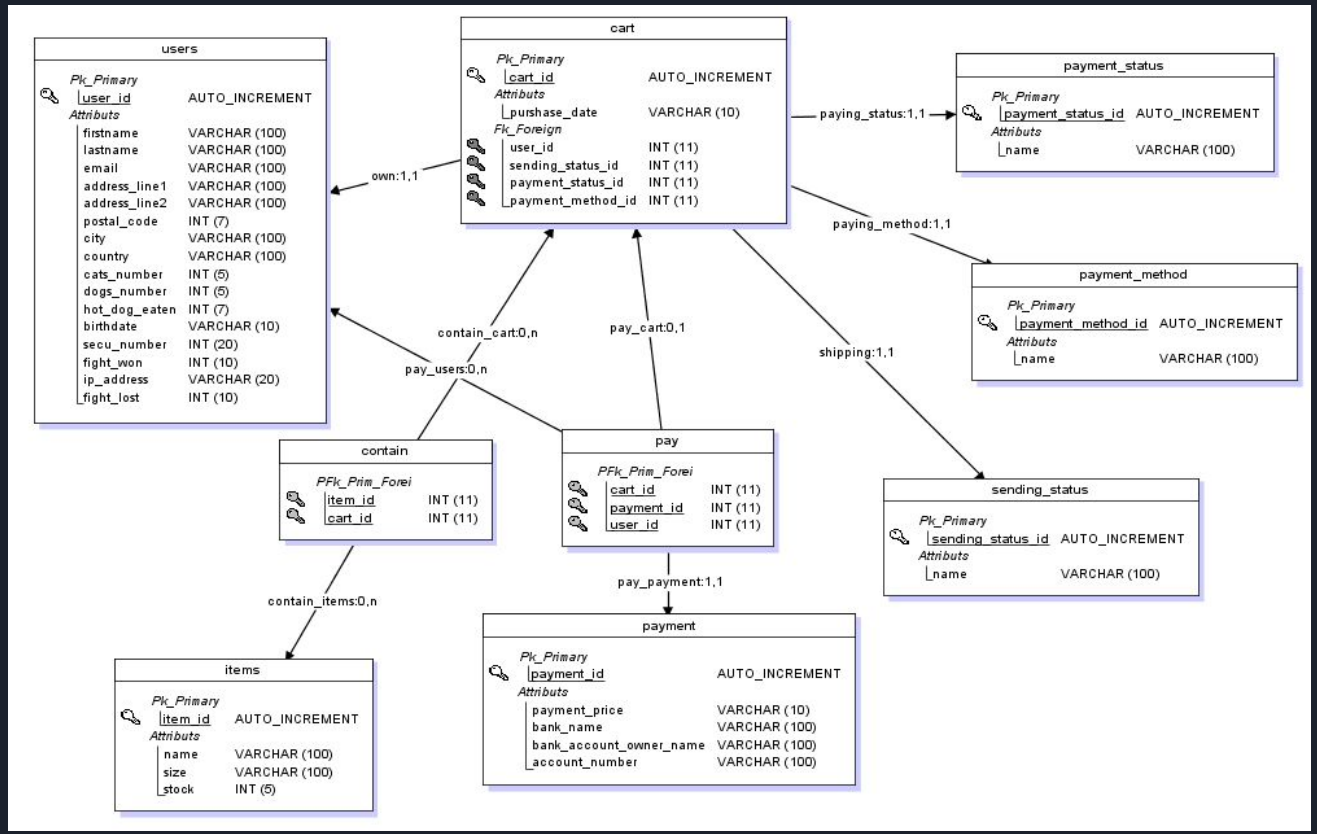
Ok un cahier des charges, mais on anonymise quoi en fait? Et c’est où ce qu’on doit anonymiser?

- Il me faut donc rechercher les données personnelles

Exercice pratique

Mais une donnée personnelle, c'est quoi?

Identifiez ce qui est une donnée personnelle dans les tables suivantes :



Exercice pratique

Quelle méthode choisir ?

Les méthodes ne sont pas exclusives les unes des autres. Vous pouvez les cumuler et les appliquer au choix selon la donnée.

Ce qu'il faut prendre en compte :

- Est-ce qu'il y a un intérêt à conserver ces données?
  - Intérêt interne : statistiques, entraînement d'un programme, historique, etc.
  - Intérêt légal : Fournir des documents comptable.
- Le coût du stockage.

Et vous dans tout ça ?

La base de données

Ce que les autres voient :

- Mine d’informations personnelles.
- Une base d'entraînement pour des programmes.
- Une cible pour des actions de masse (piratage, démarchage commercial etc.)
- L’historique et la vie de votre programme.

La base de données

Ce que vous voyez :

- Vous allez la manipuler tous les jours.
- Vous pourrez lire/modifier/récupérer des données personnelles/sensibles.
- Vous pourriez être tentés de les vendre/céder à des tiers intéressés, voire de les exploiter à des fins personnelles.

La base de données

En résumé :

- J'interagis que si nécessaire avec les données sensibles.
- Je les récupère uniquement à des fins professionnelles dans le cadre de mon emploi.
- Je ne les stocke et déplace que dans un environnement sécurisé.

Vous reprendrez bien un peu de notions de sécurité numérique ?

Sécuriser les données personnelles

Monitoring des flux :

- Suivi des requêtes sur le serveur :
  - Par l'hébergeur.
  - En interne (logs).
- Blocage des flux trop fréquents/importants (buffering).
- Gérer la surcharge du serveur (attaques DDoS).
- Suivie des actions de l'utilisateur.
- Action si comportement suspect d'un utilisateur.

Sécuriser les données personnelles

Mise à jour de la sécurité interne de l'application :

- Veille numérique (évolutions techniques + sécurité)
- Migrations (langages/framework).
- Vérification de la résistance des mots de passes.
- Protection contre les injections de code malveillant.
- Vérification des données en input.
- Utilisation de CAPTCHA.
- Gérer les temps de réponse des requêtes. (Prévenir attaques temporelles cf la vidéo de Grafikart sur le sujet).

Sécuriser les données personnelles

Sécurité interne de votre société :

- Audit sur :
  - Gestion des mots de passes.
  - Fonctionnement du réseau interne.
  - Mise à jour des ordinateurs et logiciels.
  - Réaction des salariés face aux intrusion/phishing.
  - Mise en place de processus de restauration lors du départ d'un salarié.
  - Tests blue team/red team.
- Mapping des droits :
  - Qui a accès aux données.
  - Pourquoi.
  - Comment.
  - Quelles sont ses limites.
  - Quels risques son poste peut-il générer.

Petit bonus

Éléments présents sur un site internet

CGV : De leur petit nom Conditions Générales de Vente.

A quoi ça sert à part prendre une page sur mon site?

- C’est obligatoire si le site vend un bien et/ou service.
- Informer votre client sur vos conditions de vente (produit ou prestation).
- Cadre juridique de votre vente entre le client et vous.
- Les conditions générales peuvent être complétées par des conditions spécifiques.
- Les CGV possèdent des mentions obligatoires (voir entreprendre.service-public.fr).

Éléments présents sur un site internet

CGU : pour Conditions Générales d'Utilisation.

Pourquoi faire?

- Ne sont pas obligatoires.
- Informer l'utilisateur sur le fonctionnement général du site.
- L'utilisateur doit s'y conformer pour avoir accès et utiliser votre site.
- Protéger en cas de contentieux/limiter les risques.
- Prévoir des sanctions.
- Prouver la bonne diligence du site.
- Les CGU doivent contenir :
    - La description des services/fonctionnement du site.
    - Les dispositions relatives à la propriété intellectuelle.
    - Les règles délimitant la responsabilité de l'éditeur du site.
    - Le droit applicable et les juridictions compétentes.

Éléments présents sur un site internet

Les mentions légales :

Pourquoi faire simple quand on peut faire juridique?

Il s'agit de votre carte d'identité juridique. Vous devez présenter les éléments importants de la personne (physique ou morale) derrière le site.

Nom, prénom, adresse, numéro SIRET, moyen de contact, forme juridique, etc.

Ces éléments sont décrit en détail sur la page suivante : https://www.economie.gouv.fr/entreprises/site-internet-mentions-obligatoires#

Le trademark ®™

La marque déposée : appelée trademark copyright signifie que la personne physique ou morale possède les droits d’utilisation de la marque.

Ce droit s'acquiert par l’enregistrement de cette dernière et de ses éléments constitutifs.

À défaut, la marque ne bénéficie d’aucune protection contre le vol, le détournement, l’usurpation, la copie, etc.

Le copyright ©

Le copyright : il s’agit de l’ensemble des droits de propriété intellectuelle que possède une personne sur une oeuvre de l'esprit originale.

Ce dernier n’est valable que dans les pays du Commonwealth et aux Etats-Unis.

Ce droit est différent du droit d’auteur que l’on possède en France.

Merci pour votre écoute

Merci à Objectif 3W de m’avoir permis de faire cette intervention

Pour me suivre et me contacter sur linkedin