Albert Anstett Avocat

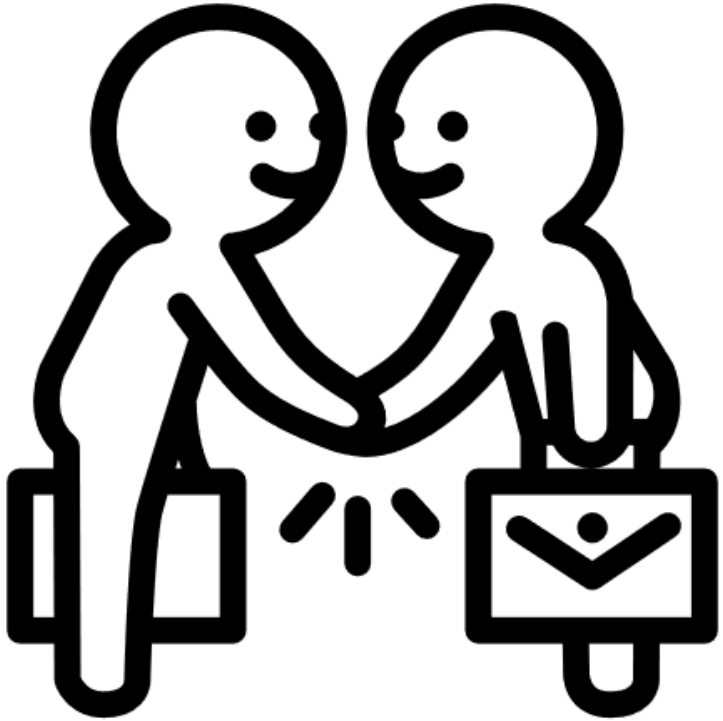
IESF
Société des Ingénieurs et Scientifiques de France

Le Règlement Général sur la Protection des Données (RGPD)

Enjeux relatifs à sa mise en œuvre par les Associations d'Alumni

- Introduction
- Principales notions
- Champ d’application
- Principales exigences
- Le RGPD en 10 questions
- Conseils pratiques

Introduction



Présentation de l'intervenant

Albert ANSTETT

- Ingénieur INSA Lyon 1993
- 23 ans dans l'industrie

  dont notamment :
  - Informatique industrielle
  - Informatique scientifique
  - Edition de logiciels
- Etudes de droit de 2008 à 2016, en parallèle de l'activité prof.
- Avocat depuis 2016
  - CIL / DPO de 10+ structures
  - Actif dans les domaines de l'industrie et du numérique

- Contacts: albert@anstett.pro, 06 37 33 94 71, LinkedIn

Le principe

- Le traitement des données à caractère personnel est strictement encadré par les normes juridiques (lois et règlement européen RGPD).

- Les organismes effectuant des traitements de données à caractère personnel doivent être en conformité avec ces règles.

- Les notions de donnée personnelle et de traitement de données sont tellement extensives qu'il n'est pas envisageable d'échapper au cadre juridique en vigueur.

L'esprit des textes

- Arbitrage entre libertés fondamentales:
  - Liberté d'entreprendre

    - Apparaît à la Révolution
    - Fondement de la **liberté** de proposer des services de traitements de données à caractère personnel

  - Droit au respect de la vie privée

    - Apparaît post-2nde guerre Mondiale
    - Fondement de la **limitation** des traitements de données à caractère personnel

- Traitement de données à caractère personnel = compromis justifié par (autorisation sous condition) :
  - Finalité du traitement

  - Consentement du titulaire ou intérêt supérieur
  - Durée de conservation

Aperçu historique

- Trois temps forts en Europe

1978

- France: Safari ou la chasse aux français

  Le Monde, 21 mars 1974

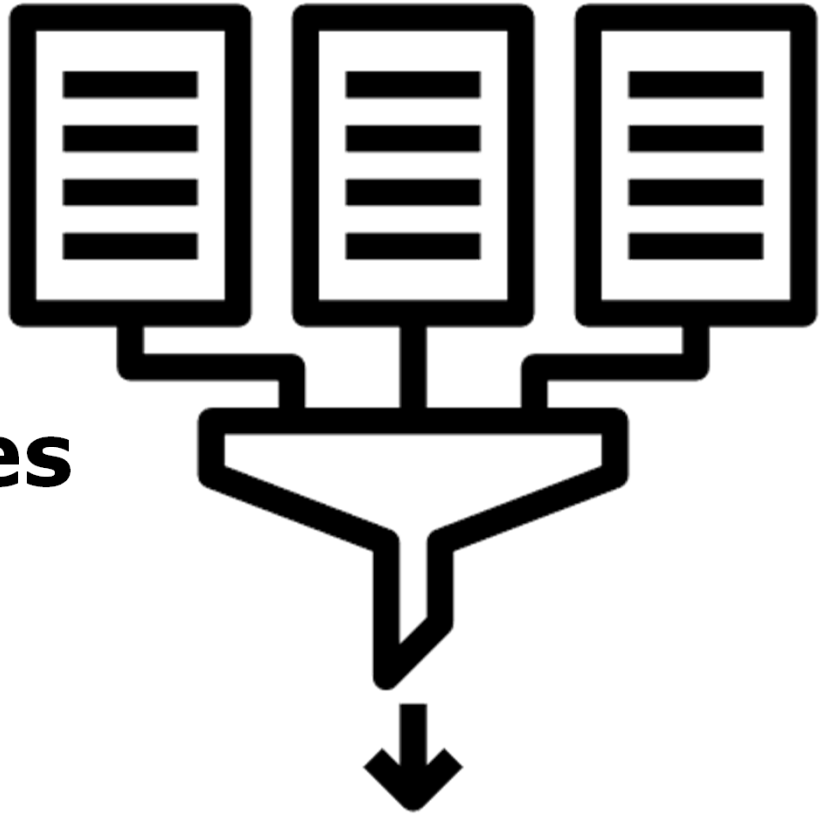
  - Un projet du gouvernement fait scandale suite à une révélation par des journalistes d'investigation du Monde
  - => Loi du 6 janvier 1978

- Europe: Directive 95/46/CE: apparition du CIL

  Transposition en France en 2004

- Europe: Règlement Général sur la Protection des Données (RGPD) => entre en vigueur le 25 mai 2018
  - Plus de droits pour les personnes
  - Harmonisation européenne

Notions principales



Donnée personnelle

Toute information se rapportant à une personne physique identifiée ou identifiable

Notion **extensive**

Titulaire

- C’est la personne physique à laquelle les données se rapportent

- C’est également la personne désignée par des recoupements d’informations à caractère personnel

- Exemples:
  - Le fils du boucher …
  - Photos des attractions dans un parc de loisirs ou une compétition sportive

Traitement de données

- Utilise des données personnelles
- Automatisé ou non
- Le fait de procéder à l'une des activités ci-dessous emporte qualification de traitement de données à caractère personnel

Collecte

Recoupement

Diffusion **Enregistrement**

Utilisation

Organisation

Extraction

Consultation

Mise à disposition

Transmission

Rapprochement

Communication **Modification**

Structuration

Conservation **Interconnexion**

Adaptation

Responsable de traitement

- La personne morale qui décide d'établir un traitement de données à caractère personnel est un **responsable de traitement**

- Le choix d'un logiciel du marché suffit à conférer la qualité de responsable de traitement

- Exemples:
  - Une association d'alumnis décide de conserver la liste de ses membres sous Excel => elle est responsable de traitement.
  - Une association d'alumnis décide de mettre en place un site internet recensant ses membres et fait appel à une offre du marché => elle est responsable de traitement

Sous-traitant

- Tout fournisseur de services intervenant pour un responsable de traitement

- Exemples:
  - NetAnswer, All In Web, …
  - OVH
  - Prestataire de service de presse (revue des alumnis)

Finalité

- RGPD => exigence de traitement licite, loyal & transparent.

- La finalité explique les raisons pour lesquelles un traitement est effectué. Elle permet de justifier le traitement.

- Respect des principes de loyauté et de transparence :
  - Consentement du titulaire
  - Traitement conforme a ce qui a été annoncé et accepté

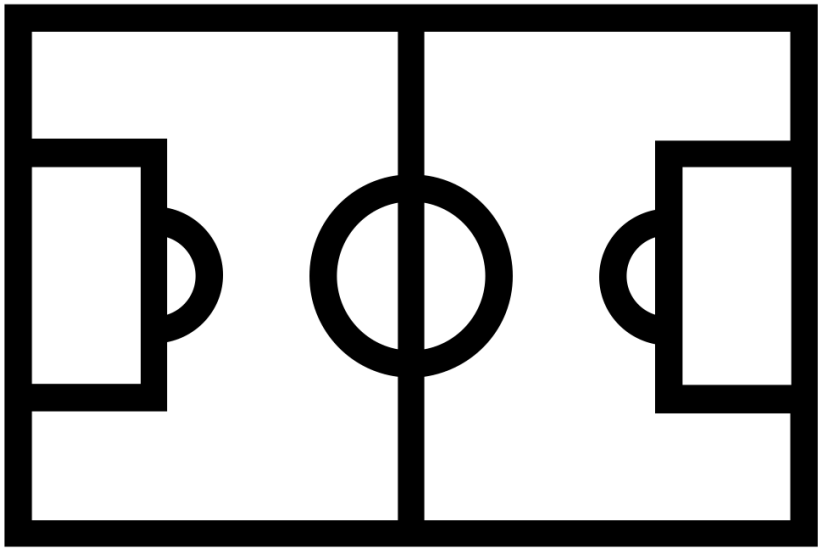
Délégué à la Protection des Données

Dans le cadre des associations d'alumni, les fonctions du DPD sont les suivantes:

- Informer le responsable de traitement sur ses obligations dans le cadre du RGPD
- Contrôler la conformité au RGPD
- Assumer un devoir de formation
- Conseiller la structure sur sa conformité au RGPD
- Etre l'interlocuteur de l'autorité de contrôle (CNIL)

La désignation est obligatoire **notamment** si:

Les activités de base du responsable de traitement consistent en des opérations de traitement qui exigent un suivi régulier et systématique à grande échelle des personnes suivies



Champ d’application

Le RGPD s'applique-t-il ?

- Champ d'application
  - géographique
  - matériel
  - temporel

Champ d'application géographique

- Le RGPD s'applique:
  - Si le responsable de traitement a un établissement au sein de l'UE.
  - Si l'un des sous-traitants a un établissement au sein de l'UE.

- Le RGPD s'applique même si le traitement a lieu en-dehors de l'UE.

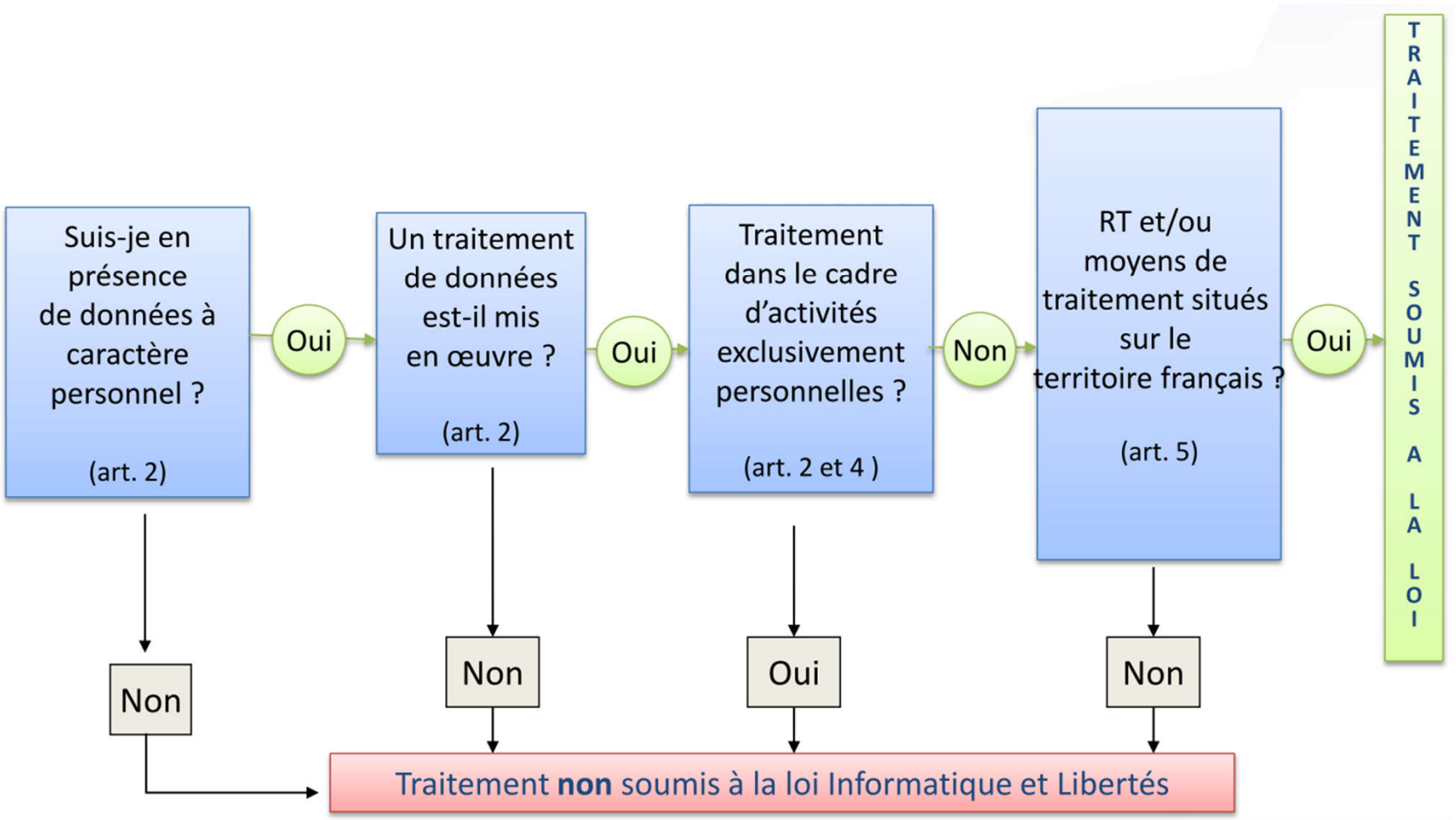
- Les responsables de traitement doivent prendre des mesures particulières en cas de sortie des données de l'UE, même à titre temporaire !

Champ d'application matériel

- Mon traitement de données est-il soumis au RGPD ?
  - Oui si le responsable de traitement est une personne morale
  - Oui si le traitement porte sur des données à caractère personnel
    - Fichier des membres
    - Fichier des contacts
    - Permanents salariés

- Dans la pratique, il est impossible de soustraire un traitement aux exigences du RGPD

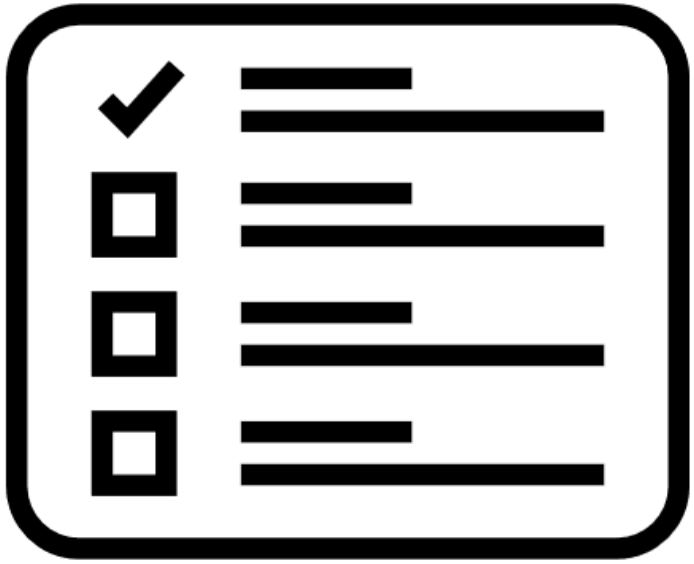
Suis-je concerné par le RGPD ?



D'après document CNIL

Champ d'application temporel

- Le RGPD est obligatoire à partir du **25 mai 2018**
- A partir de cette date, toute réclamation est traitée selon le RGPD
- A partir de cette date, les sanctions du RGPD seront appliquées



Principales exigences pesant sur les responsables de traitement

et les sanctions associées

Principales exigences pesant sur les responsables de traitement

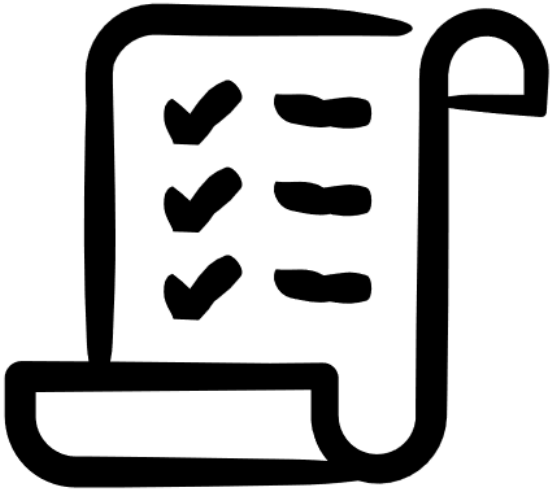
- Recueillir le consentement des titulaires au moment de la collecte des données à caractère personnel
- Collecter et traiter les données conformément à la finalité annoncée
  - ER
- Prévenir toute utilisation des données non conforme à la finalité
    - Dissémination
    - Altération
    - Destruction
    - Détournement
- Imputabilité (accountability) = obligation de moyens renforcée

Sanctions

- Sanctions pénales: inchangées / loi 1978

- Avertissement
- mise en demeure
- limitation temporaire ou définitive du traitement
- suspension des flux de données
- obligation de rectifier, limiter ou effacer, …

- amendes administratives pouvant s'élever, selon la catégorie de l'infraction, à 10 ou 20 millions d'euros.



Le RGPD en dix questions

Dix questions pour mesurer sa conformité

1. Mon association a-t-elle un fichier des membres, des adhérents, des diplômés ou des participants à une manifestation ?

2. Qui collecte les données que je traite ?
   Si c'est l'école, un consentement spécifique est nécessaire.

3. Mon personnel et mes membres sont-ils sensibilisés aux bonnes pratiques de protection des données ?
   Il est souhaitable de formaliser par des règles internes les pratiques à respecter.
   Surveillance et déclaration en cas de fuite de données.

4. Quelle est la nature des données que je collecte?
   Cas des données sensibles et des champs libres.

Dix questions pour mesurer sa conformité

5. Les finalités de mes traitements sont-elles bien définies ?
   Chaque finalité distincte fait l'objet d'un traitement spécifique.

6. Quelles procédures sont proposées aux titulaires pour l'exercice de leurs droits ? Par quelles procédures internes sont-elles mises en œuvre ?
   Droit d'accès, droit de rectification, droit à l'effacement, droit à la limitation du traitement, droit à la portabilité, droit d'opposition, cas des décisions automatiques.

7. Mon association est-elle en mesure de prouver que les titulaires des droits ont consenti aux traitements mis en œuvre ?
   Consentement en accord avec la finalité;
   Durée du consentement;
   Forme du consentement;
   Cas où les données sont collectées par l'école.

Dix questions pour mesurer sa conformité

8. Quelles sont les durées de conservation ?
   Vérifier que ces durées sont cohérentes avec les finalités.

9. Dans le cadre de mes traitements statistiques, les procédés d'anonymisation des données sont-ils robustes ?

10. En tant que responsable de traitement, mon association met-elle bien à la charge de ses sous-traitants les obligations découlant du RGPD ?
    Protection des données, sécurité;
    Limitation des traitements aux seules prestations effectivement commandées;
    Pas de sortie de l'Union Européenne;
    Obligations de déclaration en cas de perte / vol de données;
    Exigences envers les sous-traitants de rang inférieur;
    Désignation d'un DPD si nécessaire.

Mettre en œuvre le RGPD

Comment faire en pratique ?

Les premières étapes

- Recenser et décrire les traitements :
  - Finalité
  - Destinataire
  - Consentement
  - Durée de conservation
  - Types de données stockées
  - Traitements effectués
- Auditer l'activité :
  - Acteurs internes
  - Pratiques actuelles
  - Sous-traitants
- Créer un plan d'action de conformité

Rôle du DPD/DPO
Ou
En interne

Et maintenant ?

- Mutualiser les ressources pour atteindre la conformité
- Permettre la poursuite des activités
- Négocier avec les écoles