# Introduction RGPD

Règlement Général sur la Protection des Données

# Règlement Général sur la Protection des Données

- Evolution des lois Informatique et Libertés
  Loi du 6 janvier 1978, modifiée

- Protection des données personnelles, respect de la vie privée
  Article 9 du code civil :
  « Chacun a droit au respect de sa vie privée »

- Nouveaux risques, nouveaux droits, nouveaux devoirs

- Revoir les usages, se mettre en conformité

# Données personnelles

- Information permettant d'identifier une personne physique :
    - Nom, prénom,
    - Photographie, élement biométrique (empreinte, signature)
    - Adresse postale, mél ou IP,
    - Numéro de téléphone, identifiant de connexion informatique
    - Numéro de SS, d'immatriculation, de licence
    - ...

- Données sensibles pour tout ce qui peut porter à discrimination ou atteindre le respect de la vie privée :
    - Données de santé
    - Orientations politique, syndicale, religieuse, philosophique
    - Orientation sexuelle ou caractères éthniques
    - Données de traçabilité

**Accord explicite de la CNIL exigé pour toute donnée sensible**

## Notion de collecte

Collecter, c'est prendre connaissance de ces informations privées

Pas de forme privilégiée : papier ou informatique

Base légale pour la collecte :

- Intérêt vital de la personne
- Intérêt public (très encadré)
- Nécessité contractuelle
- Respect d'obligations légales
- Consentement non-ambigu de la personne
- Intérêt légitime du responsable de traitement (très encadré)

Pas de base légale, pas de collecte ...

**La notion d'intérêt étant sujette à caution, elle est très encadrée**

## RGPD – Contrôles et sanctions

- La CNIL passe du rôle de conseiller à celui de gendarme
- Recrutement d'une centaine de contrôleurs
- Priorité aux contrôles sur incidents (données commerciales)
- Secteurs sensibles → Commerce → Administrations → Associations
- Sanctions progressives, plafonds élevés (20 M€ / 4 % du budget)

⇒ Documenter les processus pour établir sa bonne foi

⇒ Anciennes déclarations CNIL remplacées par un registre obligatoire

⇒ Communiquer, expliquer, justifier

# RGPD - Obligations

- Informer préalablement à la collecte
- Recueillir le consentement à la collecte
- Limiter les données collectées au strict nécessaire
- Permettre le refus
- Protéger les données et leur usage
- Alerter
- Formaliser et documenter

## RGPD - Informer

La personne dont on collecte les données doit recevoir l'information sur :

- Qui collecte ces données (le responsable de traitement)
- Pourquoi, dans quel but (finalité du traitement)
- Pour quelle durée (échéance ou expiration)
- Quelles sont les voies de recours

**⇒ Mentions légales obligatoires**

## RGPD - Consentir

La personne dont on collecte les données doit avoir affirmé son accord pour cette collecte, sans aucune ambiguïté et après avoir pris connaissance des informations.

La collecte doit être licite et loyale :

- Licite, les informations demandées sont légitimes
- Loyale : pas d'artifice de consentement implicite

Il faut demander un consentement explicite séparé pour chaque nature de données sensibles**.**

# RGPD - Limiter

Seules les données strictement nécessaires à la finalité annoncée doivent être collectées.

La collecte de donnée superflue indique :

- Un détournement de finalité (répréhensible)
- Une finalité masquée (répréhensible)
- Une collecte indirecte ou pour un tiers (répréhensible)

La collecte pour un tiers, notamment de données sensible, doit être envisagée sous l'aspect de la confidentialité ou du secret.

**⇒ Respect de la vie privée**

## RGPD - Refuser

La personne dont les données sont collectée doit pouvoir exprimer son refus de voir ses données conservées.

Droit à l'accès, à la rectification et à l'oubli

Attention :

- La conservation des données peut parfois rester légitime
- La suppression peut avoir des conséquence
- Il faut répondre à ces demandes sous 30 jours

**⇒ Nommer un responsable de l'accès, la rectification, la suppression des données (DPO ou DPD)**

## RGPD - Protéger

Mesures de sûreté pour protéger les données et limiter les risques :

- Données accessibles aux seuls responsables de traitement
- Données utilisées exclusivement pour la finalité annoncée
- Données personnelles = privées par définition
- Consentement explicite pour la publication
- Chiffrement des transmissions / dépôts

**⇒ Responsabilisation accrue**

## RGPD - Alerter

Toute fuite de données personnelles doit faire l'objet d'une alerte dès qu'elle est constatée :

- A la CNIL pour indiquer les mesures de sécurité mises en défaut et les palliatifs employés
- Aux intéressés, en précisant la nature et la qualité des données les concernant et qui ont fuité

Contrainte lourde :

- Déclaration dans les 72h !
- Effet d'image désastreux

# RGPD - Documenter

Porter dans le registre, pour chaque traitement :

- Sa finalité :
  - Prise de licences
  - Envoi d'informations
  - Remboursements de frais
  - ...
- La nature des données concernées :
  - Données d'identification / de contact
  - Informations de gestion
  - Données bancaires
  - ...
- Les personnes concernées :
  - Membres de l'association
  - Prospects ou partenaires
- Les destinataires des informations :
  - Rôle dans l'association

# Exemple de mention légale

*Les données de ce formulaire sont nécessaire à votre inscription au club XXX et permettent la prise de licence auprès de la Fédération YYY.*

*Les informations marquées d'un (*) sont obligatoires et aucune inscription ne pourra être réalisée en leur absence.*

*Les informations marquées d'un (+) seront transmises à la Fédération et conservées selon des modalités qui lui sont propres.*

*Les informations conservées par le club le sont pendant une durée de 1 an après la saison de votre dernière inscription.*

*Conformément à la loi Informatique et Libertés du 6 janvier 1978 modifiée, vous disposez d'un droit d'accès et de rectification aux données qui vous concernent en vous adressant à Gestion.Donnees@club.fr*

☐ *En cochant cette case, je consens, explicitement, à la collecte par le club XXX des données personnelles me concernant*

*(contresignature optionnelle)*

# RGPD – Florilège chapelain (1/2)

- Employeur / Profession du licencié ou des parents
  *à éviter, ou à justifier (+ caractère optionnel)*
- Téléphone Travail
  *privilégier la collecte du téléphone portable*
- Lieu de naissance
  *quelle finalité ?*
- Taille ou poids
  *privilégier les intervalles ou catégories*
- Mentions négatives :
  - ☐ Je n'autorise pas …
  - ☐ Je refuse ...

  *déloyal. Mentions positives exclusivement*

# RGPD – Florilège chapelain (2/2)

- Numéro de sécurité sociale ***totalement interdit !!***
- Photocopie de document :pièce d'identité, justificatif de domicile ou d'assurance, ... ***privilégier le report d'information***
- Médecin traitant ***quelle finalité ?***
- Données de santé ***très délicat à gérer***
  - Théoriquement réservées aux professionnels de santé
  - Possible sous enveloppe scellée ou données portées par l'adhérent

« Renseignements complémentaires » ou « Précautions particulières »
Norme Simplifiée CNIL NS-058 applicable ?