SPORT PROPULSE FORMATION
AUVERGNE-RHÔNE-ALPES

FORMATION
Office des Sports de Lyon :

Atelier RGPD *(12/12/22)*

PLANCHE-DEFRADE Gaëtan
Chargé de missions – Juridique et Formation

Programme

PARTIE 1
Mesure des fondamentaux

PARTIE 2
Identification des principes

PARTIE 3
Plan de mise en conformité

Introduction aux questions de responsabilité

1/2

dirigeants bénévoles est **entré au CA ou au bureau par choix personnel**, par volonté de s'impliquer davantage

20%

des dirigeants bénévoles ont **déjà été confrontés à des responsabilités juridiques**

DANS 93%

des associations, **les responsabilités ne sont exercées que par des bénévoles**

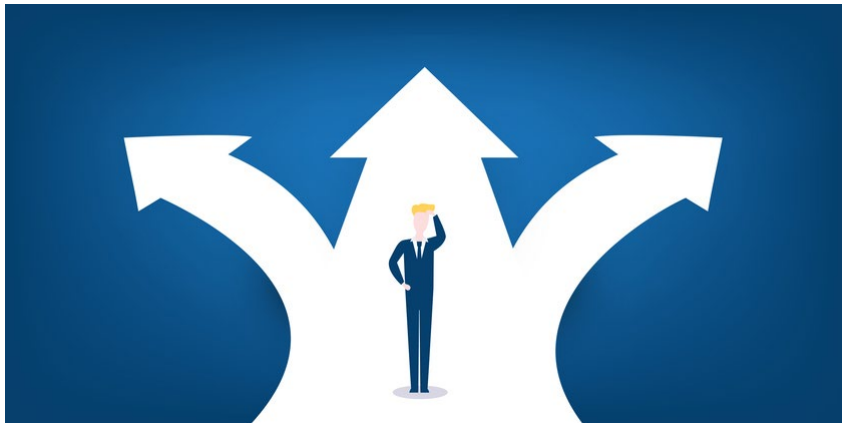
RESPONSABILITÉS LES + IMPORTANTES AUX YEUX DU DIRIGEANT BÉNÉVOLE

1. MENER À BIEN LES ACTIONS
2. VEILLER À UNE BONNE ENTENTE
3. ASSURER UNE BONNE GESTION

Le gestionnaire d'une association, bénévole ou salarié n'échappera pas à sa mise en cause lors d'une faute ayant causé un dommage.

La victime peut demander auprès du juge, chargé de trouver un responsable, la réparation des dommages matériels, physiques, financiers ou du préjudice moral.

Sa responsabilité sera **toujours recherchée mais pas forcément retenue**.



On distingue 2 grands types de responsabilité :

La responsabilité à finalité indemnitaire:
- La responsabilité civile
- La responsabilité administrative

La responsabilité à finalité répressive:
- La responsabilité pénale

Civile : Obligation de réparer le dommage causé à autrui

- **Contractuelle** : 3 conditions cumulatives **:**
Existence d'un contrat - Dommage produit pendant l'exécution – Inexécution d'une obligation d'un contractant

- Délictuelle : Principe de l'obligation de réparer tout dommage causé
Soit par sa faute, soit par celle des choses ou des animaux dont on a la garde
Soit par la faute commise par les personnes dont on est responsable

3 conditions cumulatives : un préjudice certain et direct + une faute ou un fait assimilé à l'origine
+ un lien de causalité entre le préjudice et la faute.

Administrative : **Responsabilité pour faute** :
Responsabilité liée aux pouvoirs publics, du fait des équipements sportifs,
du fait des agents publics.

Responsabilité sans faute :
Fondée sur le risque, la collaboration occasionnelle au service public.

Pénale : **Personnes Physiques**

- Faute par négligence
- Faute par imprudence
→ *Manquement à une obligation de prudence ou de sécurité*
- Imprudence caractérisée :
→ *Mise en danger délibérée de la personne d'autrui*

Personnes Morales : Nouveau Code Pénal
Depuis 1994, la responsabilité pénale des personnes morales, à l'exception d'une : L'ETAT.

SPORT PROPULSE FORMATION
AUVERGNE-RHÔNE-ALPES

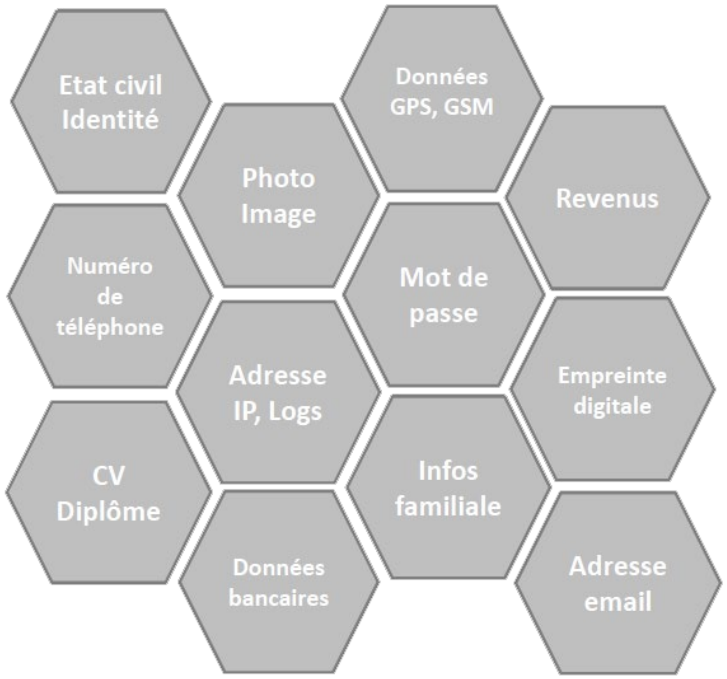
PARTIE 1 :

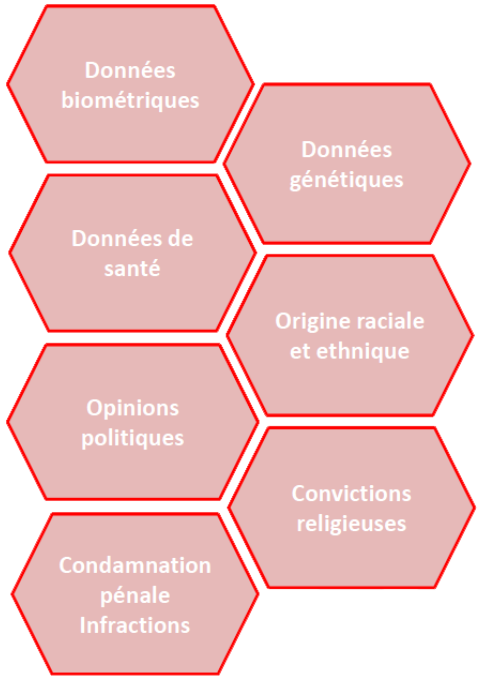
Mesure des fondamentaux

Qu’est ce qu’une donnée personnelle ?

Une donnée personnelle est toute information se rapportant à **une personne physique identifiée ou identifiable directement ou indirectement**.

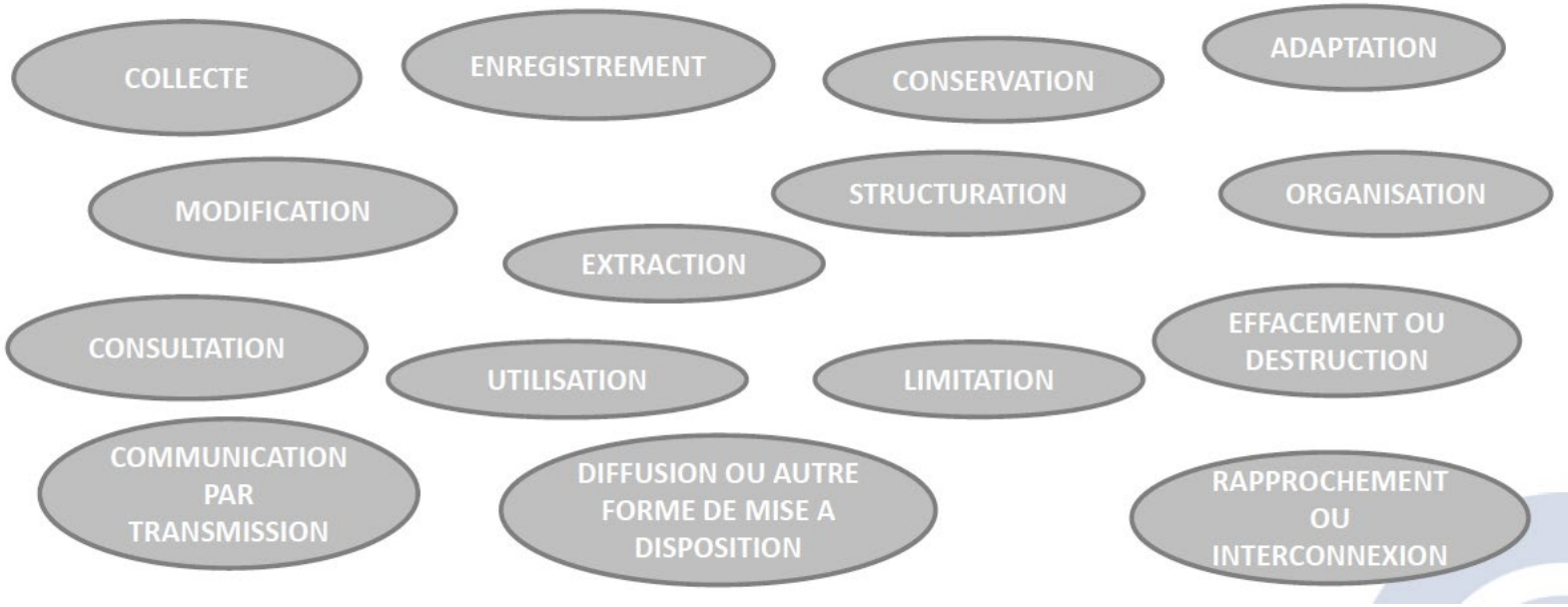
Peu importe que ces informations soient **confidentielles ou publiques.**





Qu'est-ce qu'un traitement ?

Un « traitement de données personnelles » **est une opération, ou un ensemble d'opérations**, portant sur des données personnelles, quel que soit le procédé utilisé.



Qui traite les données ?
Qui est responsable ?

Le responsable de traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement

Le sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement

Le Délégué à la Protection des Données (DPD ou DPO)

Le DPO : la personne physique externe ou interne à la structure qui organise la mise en conformité : il conseille le responsable de traitement, contrôle le respect du RGPD et coopère avec l'autorité de contrôle

Le DPO n'est **pas obligatoire dans toutes les structures**. Néanmoins, la CNIL conseille d'en désigner un (ou a minima un référent). Il peut être bénévole ou salarié et sa mission doit faire l'objet d'une désignation officielle

Quels droits possèdent les propriétaires de données personnelles ?

Droit à l'information

Avoir une **information claire** sur l'utilisation de vos données et sur l'exercice de vos droits

Droit d'opposition

S'opposer, **pour des motifs légitimes,** au traitement de ses données, sauf si celui-ci répond à une obligation légale

Droits d'accès

Obtenir les données détenues sur soi et savoir si elles font l'objet d'un traitement

Droit de rectification

Demander la rectification des informations inexactes ou incomplètes

Droit à l'effacement

Demander à un organisme l'effacement de données (selon conditions)

Droit au déréférencement

Ne plus être associé à des contenus en ligne

Droit à la limitation du traitement

Gel de l'utilisation de certaines données

Droit à la portabilité

Obtenir une copie des données ou demander au RT de les transmettre à un autre RT

Droit à l'intervention humaine

Face à un profilage ou une décision individuelle automatisée

SPORT PROPULSE FORMATION
AUVERGNE-RHÔNE-ALPES

PARTIE 2 :

Identification des principes

7 principes clefs à respecter

Principe 1 : Traitement licite, loyal et transparent

Un traitement de données personnelles ne peut être mis en œuvre sans base légale

Principe 2 : Limitation des finalités

Les données à caractère personnel doivent être collectées pour des finalités ***déterminées, explicites et légitimes****, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités*

- Le responsable de traitement devra **déterminer la finalité** de ce traitement clairement et précisément afin de prévenir tout détournement ultérieur.

- La finalité devra être légitime, c'est-à-dire répondre à un objectif du responsable de traitement et **ne pas porter atteinte aux droits fondamentaux** des personnes (même autres que la vie privée)

- Les données ne devront pas être traitées ultérieurement pour une finalité incompatible

Principe 3 : Minimisation des données

*Les données à caractère personnel doivent être **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées*

Peu importe que la donnée soit intrusive ou non, si elle n'est pas nécessaire au traitement, elle ne devra pas être collectée

Principe 4 : Exactitude

*Les données à caractère personnel doivent être **exactes** et, si nécessaire, **tenues à jour** ; toutes les **mesures raisonnables** doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.*

Principe 5 : Limitation de la conservation

Les données à caractère personnel doivent être conservées sous une forme permettant ***l'identification des personnes concernées*** *pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées*

Attention, une même donnée peut connaitre plusieurs durées de conservation différentes en fonction de la finalité du traitement mis en œuvre

Principe 6 : Sécurité

*Les données à caractère personnel doivent être **traitées de façon à garantir une sécurité** appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées*

3 types de sécurité :

- Physique (ex : mesures de protection des locaux, d'accès aux salles) ;
- Logique (ex : mesures de protection et de l'accès, mots de passe, chiffrement) ;
- Juridique (ex : contrat avec les sous-traitants).

Principe 7 : Responsabilité et preuve

Le responsable du traitement *est responsable du respect des 6 principes précédents et est en mesure de démontrer que celui-ci est respecté.*

Il s'agit donc :

- D'être conforme à la règlementation ;
- De démontrer la conformité à la règlementation.

Exemples : Contrats sous-traitants, clause de confidentialité dans les contrats, politique de confidentialité, registre des activités de traitements, codes de conduite, procédures diverses…

Quelles sont les sanctions ?

Cas de sanction	Sanction maximale
Le **délit d'entrave** en cas de contrôle est une volonté manifeste du RT de ne pas coopérer ou de dissimuler des informations.	1 an d'emprisonnement et 15 000€ d'amende
Sanction administrative niv. 1 en cas de : - Faille de sécurité (Art. 32 à 34) - Traitement impliquant le consentement des enfants (Art. 8) - Traitement ne nécessitant pas l'identification (Art. 11) - Analyse d'impact et DPO (Art. 25 à 39) - Certification (Art. 42 et 43) - Suivi des codes de conduite (Art. 83 §4)	2% du chiffe d'affaire annuel mondial ou 10M€ (Les Etats membres fixent les amendes pour les organismes publics.)
Sanction administrative niv. 2 en cas de : - Non respect des droits des personnes concernées - Les transferts de données hors UE - Non respect d'une injonction ou d'une limitation temporaire ou définitive d'un traitement - Refus de donner accès à un traitement à l'autorité de contrôle	4% du chiffre d'affaire annuel mondial ou 20M€ pour les organismes privés (Les Etats membres fixent les amendes pour les organismes publics.)

SPORT PROPULSE FORMATION
AUVERGNE-RHÔNE-ALPES

PARTIE 3 :

Plan de mise en conformité

ETAPE 1 : Établir un plan d'actions

- **Former un groupe de travail**
- **Définir les grandes tâches et les sous-tâches**
- **Réaliser un rétroplanning réaliste**
- **Définir les rôles de chacun en fonction du temps libre, des compétences de chacun**

ETAPE 2 : Garantir aux personnes l'information et l'application de leurs droits

- **La création d'une adresse email dédiée**
  Mailo, Protonmail, Tutanota…
- **Les mentions d'information**
- **La Politique de protection des données / de confidentialité**
  Document récapitulant les différents modes de collecte et de traitement des données réalisés sur le site
- **Une procédure de gestion des droits des personnes**
  Document interne qui définit les différentes étapes lors de la demande d'application de droits
  > Registre des demandes des personnes concernées
- **La mise en place d'un plug-in Cookies**

ETAPE 3 : Recueillir et prouver le consentement éclairé

- **Formulaire de collecte de données faisant apparaître le consentement**
  > Papier ou numérique, toujours garder une preuve du consentement
  > Cette preuve est à conserver le temps que vous détenez les données

- **Outils newsletter**
  Envoyer une campagne à tous les contacts pour lesquels vous n'avez pas obtenu d'opt-in

ETAPE 4 : Organiser et justifier le stockage des données

- **Procédure de durées de conservation**
  Document interne qui définit les différentes durées de conservation
  > Minimiser autant que possible les durées en fonction de la finalité

- **Procédure de stockage des données**
  Document interne qui définit les modes et lieux de stockage en fonction des données collectées

- **Registre des activités de traitement**
  Document interne de recensement et d'analyse de l'ensemble des traitements
  C'est aussi un outil de pilotage et de démonstration de votre mise en conformité

ETAPE 5 : Garantir la sécurité des données

- **Contrats sous-traitants**
  Clauses à prévoir dans les contrats
- **Charte informatique**
  Document qui définit les conditions générales d'utilisation des systèmes d'information et de communication, de l'accès à Internet…
- **Registre des habilitations**
  Document interne qui définit les habilitations en fonction des fichiers de données
- **Politique de sécurité des systèmes d'information**
  Document définissant la stratégie de sécurité de la structure
- **Procédure faille sécurité et notification à la CNIL**
  Document interne qui définit la procédure à suivre en cas de faille de sécurité
  > Registre des violations

ETAPE 6 : S'organiser en interne pour intégrer le RGPD

- **Procédure de Privacy by design**

  Document interne qui définit de quelle manière est intégré le RGPD dans chaque nouveau projet de la structure

- **Formations en interne et registre des formations**

  La sensibilisation et la formation des salariés et bénévoles fait partie intégrante de la preuve de votre conformité au RGPD

ETAPE 7 : Anticiper un contrôle de la CNIL

- **Procédure en cas de contrôle CNIL sur place/en ligne/à distance**

Document interne qui définit la procédure à suivre en cas de contrôle de la CNIL (acteurs, étapes…)

- **La plupart des contrôles sont réalisés à la suite d'un signalement**

Pour manquement aux différents principes énoncés

Bilan du RGPD 3 ans après

Les chiffres clés : Rapport d'activité 2020 de la CNIL

13 585 plaintes de la part d'internautes et 38 799 depuis la mise en place du RGPD

40% des contrôles suite à une plainte ou signalement

Un montant total d'amendes de **138 M €** en 2020

61% des organismes soumis au RGPD collectent plus ce que la loi leur permet

77% des organismes ne sont pas sûrs d'avoir que des données clients nécessaires

SPORT
PROPULSE
FORMATION
AUVERGNE-RHÔNE-ALPES

CONCLUSION :

Temps d'échanges