# NUMERIQUE ASSOCIATIF
# Atelier RGPD

**Contexte :** *Depuis le 25 mai 2018, le Règlement Général sur la protection des données (RGPD) est entré en vigueur afin de renforcer la loi « Informatique et libertés ». Les associations loi 1901 sont contraintes, au même titre que toute organisation, de se mettre en conformité avec les nouvelles règles. Face à l'ampleur de la tâche et au manque de moyens humains et de compétences, cette mise en conformité est à ce jour réalisée par très peu d'associations du territoire. Le CROS AURA propose ainsi une formation permettant aux participants d'en comprendre les principes et les enjeux.*

---

**Objectifs Pédagogiques :**
*> Connaitre et comprendre les principes du RGPD en présentant les éléments de preuves adéquats ;*
*> Connaître et maîtriser les droits des personnes en matière de protection des données personnelles ;*
*> Connaître les risques encourus en cas de non-respect et savoir comment répondre aux exigences.*

---

## Introduction aux questions de responsabilité :

### RESPONSABILITE DE L'ASSO ET DE SES ACTEURS

**Introduction :** On distingue 2 grands types de responsabilités :

1. **La responsabilité à finalité indemnitaire : responsabilité civile et administrative.** Le but est ici d'obtenir la réparation du préjudice subi par la victime par l'allocation de dommages et intérêts. Elle est engagée devant les juridictions civiles quand l'accident concerne 2 personnes privées, ou bien devant les juridictions administratives quand une personne publique est impliquée.

2. **La responsabilité à finalité répressive : responsabilité pénale.** Le but est ici de faire prononcer par le juge pénal, au nom du peuple français, la condamnation d'une personne à une amende ou une peine privative de liberté, ou encore à une peine complémentaire. Pour l'engager, une infraction pénale (contravention, délit, crime) doit avoir été réalisée.

**Principe** : Le juge civil répare le dommage subi et le juge pénal sanctionne l'auteur du dommage. Nous sommes donc en présence de 2 responsabilités aux finalités différentes mais qui peuvent se cumuler lorsque la victime de l'accident engage plusieurs chefs de responsabilités.

**Spécificité des règles de droit. Droit commun.** En matière sportive, il existe peu de règles de droit spécifiques (Code du sport) et ce sont les règles du droit commun qui s'appliquent. En cas de litige ou d'accident, les parties saisissent les juridictions pour obtenir réparation de leur dommage. En matière sportive, il n'existe pas de juridiction spécialisée pour trancher les litiges sportifs donc ce sont les juridictions de droit commun.

## *La responsabilité civile*

**Définition.** Elle se définit comme l'obligation de réparer le dommage causé à autrui. Tout agissement qui cause un dommage à autrui peut donner lieu à réparation. La responsabilité civile consiste pour la victime à faire reconnaître par le juge civil qu'un dommage lui a été illégitimement causé et qu'à ce titre son auteur lui en doit réparation sous la forme de l'allocation de dommages et intérêts. Ces dommages et intérêts représentent le montant estimé du dommage causé.

**Responsabilité contractuelle.** Elle est définie aux articles 1231 et suivants du Code civil et pose le principe d'une réparation d'un dommage subi en raison de l'inexécution ou de la mauvaise exécution d'un contrat. Trois conditions cumulatives doivent être réunies, à savoir : **Une faute.** On parlera de « faute contractuelle » et il s'agira de rechercher l'existence d'un manquement à une obligation née du contrat. **Un préjudice.** Qu'il soit matériel, corporel ou moral, le préjudice doit avoir été réalisé pendant l'exécution du contrat pour pouvoir être indemnisé. Direct et certain, le dommage doit avoir été causé par l'un des contractants, à l'autre, du fait d'inexécution ou mauvaise exécution. **Un lien de causalité.** Il doit exister une relation de cause à effet entre la faute et le dommage.

**Moyens de défense.** Trois causes d'exonération de responsabilité peuvent être invoquées par celui qui voit sa responsabilité engagée : la force majeure, le fait de la victime et le fait d'un tiers (se reporter au Code civil pour des exemples de solutions jurisprudentielles).

**Obligation de sécurité**. Dans le cadre de l'exercice de leur activité, les gestionnaires de club ou d'un service sportif, les dirigeants de structures ainsi que les personnels dédiés, qu'ils soient bénévoles, salariés ou fonctionnaires, sont assujettis au respect de cette obligation très contraignante. Elle découle directement des règles de droit commun et de règles spécifiques. Il s'agit en particulier d'une obligation d'origine contractuelle dont le non-respect (inexécution ou bien mauvaise exécution) sera susceptible d'engager la responsabilité contractuelle de la personne qui en est débitrice. Ce sont les tribunaux qui, dans chaque espèce, déterminent les contours des obligations de sécurité propres à chaque type d'activités. Cela signifie aussi que, si le gestionnaire respecte les règles de l'art et les règles techniques de la discipline, les hypothèses où le juge retiendra sa responsabilité seront rares.

**Nature de l'obligation**. Elle sera tantôt une obligation de moyens, tantôt une obligation de résultat, avec ce que cela entraîne comme conséquences. La différence entre l'obligation de sécurité de résultat et de moyens tient essentiellement à l'intensité de ce qui est attendu du cocontractant et au rôle plus ou moins actif (obligation de moyens) ou passif (obligation de résultat) de l'usager. L'obligation de moyens oblige le contractant à mettre en œuvre tous les moyens dont il dispose pour parvenir à un résultat sans y être tenu. L'obligation de résultat signifie que le contractant est tenu de parvenir au résultat, donc la charge de la preuve incombe à l'organisateur.

**Responsabilité délictuelle.** Les régimes de la responsabilité civile délictuelle sont de cinq ordres, contenus aux articles 1240 à 1244 du Code civil. Pour mémoire, il s'agit de la responsabilité du fait personnel, du fait d'autrui, du fait des choses, du fait des animaux et du fait des bâtiments. Est ainsi posé le principe de l'obligation de réparer tout dommage causé.

**Mise en œuvre.** Trois conditions cumulatives doivent être réunies. **Une faute.** Pour rappel, elle peut être volontaire ou involontaire. Concernant la faute involontaire, pour imprudence ou négligence, il appartient au juge d'apprécier le comportement de l'auteur du fait à celui d'un homme « très diligent » placé dans les mêmes circonstances et de la même condition sociale. **Un préjudice.** Qu'il soit matériel, corporel ou moral, le préjudice doit avoir été réalisé pour pouvoir être indemnisé. Par exception, il est admis que la réparation d'un préjudice futur puisse être prise en compte si sa réalisation est certaine et son évaluation possible. **Un lien de causalité.** Il doit exister une relation de cause à effet entre la faute et le dommage, le préjudice indirect ne pouvant donc pas être indemnisé en principe.

**Moyens de défense.** Trois causes d'exonération de responsabilité peuvent être invoquées par celui qui voit sa responsabilité engagée : la force majeure, le fait de la victime et le fait d'un tiers. A ce titre, les responsabilités encourues par les sportifs à l'occasion de leurs activités relèvent bien du régime de la responsabilité délictuelle.

# *La responsabilité administrative*

Les activités sportives peuvent engendrer la mise en jeu de la responsabilité administrative de l'Etat ou des collectivités lorsque des dommages ont été occasionnés. Cela peut faire suite à la mauvaise organisation d'activité sportive, par l'équipement public sportif qu'elles mettent à la disposition du club ou encore par l'ensemble des pouvoirs de police dont dispose l'autorité de police. Comme en matière civile ou pénale, il se trouve que la responsabilité administrative est engagée lorsqu'il existe une faute, mais que dans quelques cas très restrictifs, elle peut être engagée même en l'absence de faute.

## 1 : Responsabilité pour faute

Il est question de faute lorsqu'une action ou une abstention de l'État, d'une collectivité publique, d'une collectivité territoriale, porte préjudice à un administré. Les droits de ce dernier ayant été atteints, une demande préalable indemnitaire puis une procédure contentieuse peuvent alors s'ouvrir. Le préjudice peut s'apprécier de diverses manières. Il peut s'agir de l'illégalité d'une décision administrative (résultant d'un arrêté, décret, d'une loi, délibération, etc.), ayant eu pour effet de priver un administré d'un droit dont il aurait pu bénéficier ; il peut être également question de l'abstention des forces publiques en cas de troubles à l'ordre public ou encore d'un ouvrage public mal entretenu.

La responsabilité administrative est graduelle : de la faute simple à la faute lourde. Dans le cadre de la faute lourde, pour pouvoir engager la responsabilité de l'administration, il faut que cette faute soit d'une particulière gravité, tandis que pour la faute simple, comme son nom l'indique, un simple manquement suffit. Cependant, aujourd'hui la faute lourde est en net recul, ce qui signifie que la faute simple suffit généralement pour engager la responsabilité de l'administration.

## 2 : Responsabilité sans faute

Elle tire sa source d'une jurisprudence, l'arrêt Cames du 21 juin 1895. Elle prend le contre-pied de la responsabilité administrative pour faute, puisqu'à l'origine, après l'arrêt Blanco de 1873, la puissance publique n'était responsable que pour des fautes de service.

Pour des raisons d'équité, la responsabilité administrative sans faute voit le jour, pour permettre aux administrés de pouvoir être indemnisés plus facilement, sans avoir à rapporter une quelconque preuve de la faute commise par l'administration, lorsque l'administration fait peser sur ce dernier, dans l'exercice normal de son activité, un risque pouvant lui occasionner des dommages. C'est le cas lorsqu'il est exposé à une chose ou activité dangereuse, par l'administration ou un de ses collaborateurs du service public, dans le cas où ce dernier aurait exécuté sa mission sous demande de l'administration. Dans ce dernier cas, l'administration est également responsable du fait de son collaborateur du service public.

# *La responsabilité pénale*

**Définition.** C'est l'obligation pour une personne de répondre des infractions qu'elle commet, que ce soit dans le cadre d'une contravention, d'un délit ou d'un crime. En ce qui concerne l'organisation d'activités ou d'événements sportifs, les infractions concernent le plus souvent les 2 premières catégories, mettant en jeu l'intérêt public. Elle a une fonction de répression, ayant pour objet de désigner juridiquement et socialement un coupable qu'il convient de punir, notamment en lui infligeant une amende ou une peine privative de liberté et éventuellement une peine complémentaire.

**Qualité des personnes poursuivies.** Depuis 1994, les nouvelles dispositions du code pénal permettent de poursuivre les personnes morales (collectivités, sociétés, associations, clubs, fédérations, etc.), au même titre que les personnes physiques (dirigent, président de club, entraîneur, organisateur, etc.) dès qu'elles commettent une infraction (Art L.121 du Nouveau Code Pénal). Elles encourent des sanctions spécifiques d'amende ou sanctions adaptées pour les infractions qu'elles commettent (montant généralement porté au quintuple de celui des personnes physiques).

**Cumul de responsabilité civile et pénale :** Dans la même instance, la victime du dommage peut demander au juge pénal de se prononcer à la fois sur l'action pénale (répression) et sur l'action civile (réparation, octroi de dommages et intérêts). Cette double action devant le juge répressif lui permet de n'engager qu'une seule procédure et de confier à un juge d'instruction la charge du procès.

**Incriminations pénales. Diversité.** Toute personne peut être déclarée pénalement responsable des infractions prévues par la loi, c'est-à-dire par le code pénal. Il existe plusieurs catégories d'incriminations pénales de droit commun applicables en matière sportive, et des incriminations pénales spécifiques au sport, c'est à dire créées spécifiquement pour les différents acteurs sportifs.

On note que l**es atteintes volontaires à la personne** comprennent les atteintes volontaires à la vie et à l'intégrité physique. En revanche, les atteintes volontaires à l'intégrité physique correspondent à des violences ayant entraînées la mort sans intention de la donner, une mutilation ou une ITT.

**Les atteintes involontaires à la personne**. La responsabilité pénale est ici engagée en raison d'une faute de maladresse, de négligence, d'imprudence, etc. permettant d'imputer à son auteur un résultat qu'il n'a pas souhaité. Ainsi, l'homicide involontaire est constitué quand la mort d'autrui a été causée par maladresse, imprudence, inattention, négligence ou manquement à une obligation de sécurité ou de prudence. De même, des blessures par imprudence sont constituées lorsqu'elles sont le résultat d'un comportement d'imprévoyance.

**La mise en danger de la vie d'autrui**. L'article 223-1 du Code pénal la définit comme « le fait d'exposer directement autrui à un risque immédiat de mort ou de blessure de nature à entraîner une mutilation ou une infirmité permanente par la violation manifestement délibérée d'une obligation particulière de sécurité ou de prudence imposée par la loi ou le règlement ».

**Délit de non-assistance de personne en danger**. Ce délit est constitué quand on ne prête pas secours à une personne en péril dès lors qu'il n'existe aucun danger pour soi, pour les autres participants et pour le groupe que l'on accompagne.

# PARTIE 1 : Mesure des fondamentaux

## Qu'est-ce qu'une donnée personnelle ?

La notion de « données personnelles » est à comprendre de façon très large

L'identification d'une personne physique peut être réalisée :
• à partir d'une seule donnée
• à partir du croisement d'un ensemble de données

Les données sensibles sont régies spécifiquement soit sous **forme d'interdiction** de leur collecte soit sous **forme d'obligation** particulière de gestion.

**Au sens réglementaire, les données sensibles visent** les exemples suivants.

Il est par principe interdit de recueillir ou d'utiliser ces données sensibles, sauf exceptions :
• *si la personne concernée a donné son consentement exprès ;*
• *si les informations sont manifestement rendues publiques par la personne concernée ;*
• *si elles sont nécessaires à la sauvegarde de la vie humaine ;*
• *si leur utilisation est justifiée par l'intérêt public et autorisée par la CNIL ;*
• *si elles concernent les membres d'une organisation politique, religieuse, syndicale…*

En pratique : il convient d'éviter la collecte de données sensibles, excepté si votre activité l'exige auquel cas vous devrez **vous assurer de la licéité du traitement**. Dans un tel cas, ne collectez que celles strictement nécessaires, avec une gestion spécifique d'accès restreint et de sécurité informatique accrue, pour une **durée de conservation strictement nécessaire** à la poursuite du motif ayant justifié votre collecte entrant dans le champ d'exceptions.

## Qu'est-ce qu'un traitement ?

Un fichier ne contenant que des coordonnées d'entreprises n'est pas un traitement de données personnelles. Un traitement de données personnelles **n'est pas nécessairement informatisé** puisque les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions. **Un traitement de données doit avoir un objectif, une finalité**, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour. À chaque traitement de données doit être assigné un but, qui doit bien évidemment être **légal et légitime au regard de votre activité** professionnelle.

## Qui est responsable ?

Le sous-traitant est la personne à laquelle le responsable de traitement délègue la mise en œuvre du traitement ou une partie de celui-ci en respectant les instructions que celui-ci lui fournit (prestataires de services informatiques, prestataires de paie, équipementiers…)

## Le Délégué à la Protection des Données

Il peut être bénévole ou salarié et sa mission doit faire l'objet d'une désignation officielle, via une lettre de mission pour le salarié, une convention pour le bénévole.

Attention, la désignation d'un DPO auprès de la CNIL implique le respect de plusieurs obligations : formation, accès aux informations, indépendance fonctionnelle et ressources nécessaires à la mission, secret professionnel, confidentialité

**3 cas où la nomination du DPO est obligatoire** :

- Les traitements sont effectués par une autorité publique (ou un organisme public)
- Les activités de base de l'organisme consistent en des opérations de traitement exigeant un suivi régulier et systématique à grande échelle des personnes concernées
- Les activités consistent en un traitement à grande échelle de données sensibles

## Les droits des titulaires de données personnelles

**- Droit à l'information**
Obtenir une info précise sur la collecte et le traitement des données
Premier baromètre pour déterminer le **degré de confiance** à accorder à un organisme.

**- Droits d'accès**
Vous pouvez demander à un organisme s'il détient des données sur vous (site web, magasin, banque...) et demander à ce que l'on vous les **communique pour en vérifier** le contenu.

**- Droit de rectification**
Vous pouvez demander la rectification des **informations inexactes ou incomplètes** vous concernant. Il permet d'éviter qu'un organisme n'utilise ou ne diffuse des infos erronées.

**- Droit d'opposition**
Toute personne a le droit de s'opposer, **pour des motifs légitimes,** au traitement de ses données, sauf si celui-ci répond à une obligation légale Le droit d'opposition vous permet de vous opposer à ce que vos données soient utilisées par un organisme pour un objectif précis.

**- Droit à l'effacement**
Vous avez le droit de demander à un organisme **l'effacement de données** à caractère personnel vous concernant.

**- Droit au déréférencement**
**Ne plus être associé à des contenus en ligne**. Le déréférencement permet de faire supprimer un ou plusieurs résultats fournis par un moteur de recherche à l'issue d'une requête effectuée à partir de l'identité (nom et prénom) d'une personne. Pour supprimer l'information sur le site source, privilégiez une demande auprès du responsable du site**.**

**Droit à la limitation du traitement**
Gel de l'utilisation de certaines données. Le droit à la limitation de vos données est un droit qui complète vos autres droits (rectification, opposition...). Si vous contestez l'exactitude des données utilisées ou que vous vous opposez à ce que vos données soient traitées, la loi autorise l'organisme à procéder à une vérification et pendant ce délai, vous avez la possibilité de demander à l'organisme de ne plus les utiliser les données mais devra les conserver.

**Droit à la portabilité**
Obtenir une copie des données ou demander au RT de les transmettre à un autre RT
Avec le droit à la **portabilité** des données, vous pouvez demander à récupérer les données que vous avez fournies à une plateforme, pour un usage personnel ou pour les transmettre.

**Droit à l'intervention humaine**
Face à un profilage ou une décision individuelle automatisée. Le profilage consiste à utiliser les données personnelles d'un individu en vue d'**analyser et de prédire son comportement**, impliquant l'établissement d'un profil individualisé relatif à une personne.

---

## PARTIE 2 : Identification des principes

## Comment traiter les données personnelles dans les règles ?

***Principe n1 : Traitement licite, loyal et transparent***

**Sur le principe de collecte loyale** : la **personne concernée doit être informée de l'existence et des finalités du traitement, ainsi que des conséquences** en cas de refus du traitement. Plus loin, le RGPD, mentionne également deux obligations qui y sont liés, à savoir l'obligation de finalités « déterminées, explicites et légitimes », ainsi qu'un traitement « adéquat, pertinent et limité » des données.

**Sur l'obligation de transparence** : elle se compose en partie du droit à l'information, qui consiste à permettre à l'utilisateur de demander d'être informé sur les traitements dont ses données personnelles font l'objet, ainsi que de **pouvoir être informé** de **la finalité et des modalité**s du traitement. Ce droit ne peut donc normalement pas être opposé à une personne qui doit ainsi savoir si la collecte est directe ou indirecte. Enfin, l'obligation est également constituée d'un **volet concernant l'utilisation des données**.

**Sur la licéité du traitement** : le principe consiste en une liste précisant les cas de licéité, le premier impliquant que l'utilisateur ait donné son consentement pour une ou plusieurs finalités définies et spécifiques. Il s'agit d'un **consentement positif** où l'utilisateur précise, pour chaque donnée, et chaque finalité, son choix concernant cette donnée personnelle. Notons que **le choix de l'utilisateur ne peut en aucun cas altérer** son utilisation du service.

Le consentement n'est pas forcément la base légale privilégiée lors d'un traitement, puisque le législateur prévoit de nombreuses exceptions

***Principe n2 : Limitation des 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

- 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***
La CNIL n'est pas claire sur les durées de conservation. A partir de ce moment-là il convient à chacun de déterminer des durées de conservation raisonnables et justifiables au regard de la finalité du traitement. L'important est de toujours pouvoir justifier cette durée.

3 types de conservation :

- Les bases actives ou archives courantes : données d'utilisation courante
- Archives intermédiaires : donnée pour laquelle le traitement a pris fin mais qui peut encore servir administrativement (respect obligation légale, se prémunir d'un contentieux, réaliser un contrôle interne…). Doivent être conservées sur un support distinct et consultées de manière ponctuelle et motivée.
- Archives définitives : organismes publics

***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*

***Principe 7 : Responsabilité et preuve (nouveau principe)***

On pourrait ajouter un 8ème principe, qui est celui du Privacy by design.
Celui-ci consiste à inclure la protection des données dès la réflexion d'un nouveau projet.
C'est-à-dire être dans une démarche pro-active et préventive.

## Chapitre 4 : Sanctions et bilan

Au titre des sanctions : la CNIL sanctionne chaque année entreprises et institutions pour leurs manquements au RGPD avec un montant de **sanctions pécuniaires** pouvant s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du CA annuel mondial. Ces sanctions peuvent également être rendues publiques, principalement pour :

- des données rendues accessibles à des tiers sans autorisation ;
- des manquements concernant l'information et le traitement des données de clients potentiels
- des manquements relatifs aux cookies et à l'obligation de limiter la conservation
- une insuffisante protection et sécurité des données personnelles d'utilisateurs
- un envoi massif de courriels sans preuve de consentement préalable

# PARTIE 3 : Plan de mise en conformité

**La mise en conformité au RGPD**

## Etape 1 : Etablir un plan d'actions de la mise en conformité

La première étape est de définir un plan d'actions qui détaille et planifie les étapes suivantes.

## Etape 2 : Garantir aux personnes physiques l'information et l'application de leurs droits

### 1. Création d'une adresse email dédiée

Conseil : utiliser un fournisseur éthique et qui respecte le RGPD

- Mailo (hébergé en France)
- Protonmail (messagerie chiffrée / hébergé en Suisse)
- Tutanota (hébergé en Allemagne / chiffrage possible / open source)

### 2. La mention d'information

Répond au droit d'information des propriétaires de données personnelles
Obligatoire à chaque collecte de données personnelles.
L'information doit être rédigée simplement, de manière claire et lisible.

https://www.cnil.fr/fr/exemples-de-formulaire-de-collecte-de-donnees-caractere-personnel

### 3. La politique de protection des données

A faire apparaitre en bas de page du site internet avec les mentions légales et les CGU du site (deux documents obligatoires) pour **porter à la connaissance des personnes dont vous collectez et détenez des données un certain nombre d'informations**

Concrètement, vous devez :
- établir votre Politique de Confidentialité,
- créez une rubrique « Politique de Confidentialité » accessible depuis votre page web,
- rendre la politique accessible depuis la rubrique,
- faire accepter, lors de la création d'un compte client, par un consentement en opt-in

**NB : Votre site internet est important à sécuriser car :**
- Il est le reflet de votre niveau d'investissement sur le RGPD
- C'est un formidable outil d'information par sa facilité d'accès
- C'est un point central à la collecte des données personnelles utiles à votre activité
- C'est un formidable outil probatoire très simple à contrôler pour la CNIL

*En 2020, 33% des contrôles de la CNIL se sont fait en ligne (Rapport d'Activité CNIL 2020)*

### 4. Procédure de gestion des droits des personnes

Dans cette procédure il faudra inscrire où et sous quelle forme devront être stockées les preuves de la demande et de la réponse. + registre des demandes des personnes concernées
**C'est une obligation essentielle** : **vous devez impérativement donner suite** (ou justifier pourquoi vous ne donnez pas suite légitimement) à une demande d'exercice d'un droit. Le délai légal pour répondre à une demande d'application d'un droit est de 1 mois sauf le droit à rectification qui doit être traité « dans les meilleurs délais ».

En pratique… Vos clients et prospects doivent pouvoir exercer leurs droits directement sur votre site web depuis une rubrique ou auprès d'une **boîte mail dédiée**. C'est une preuve de sérieux et d'engagement à l'objectif majeur du RGPD

### 5. Cookies

Faire la demande à votre webmaster ou à la personne qui a créé votre site ou réalise sa maintenance. Il s'agit d'installer un **plug-in ou module d'extension** qui gère le consentement des personnes et le dépôt de cookies sur leur ordinateur en fonction des préférences qu'ils auront définies. **La CNIL a publié récemment des recommandations** que vous pouvez communiquer à la personne qui gère votre site.

https://www.cnil.fr/fr/cookies-et-traceurs-comment-mettre-mon-site-web-en-conformite

Il faut respecter la même exigence pour les cookies et pour la collecte de données personnelles, soit le **recueil du consentement actif** de l'utilisateur pour des finalités précises.

Ce consentement doit être libre, spécifique, éclairé, univoque et retirable. Concrètement… Pour recueillir le consentement, mettez en place **un bandeau de cookies sur la page d'accueil** du site web. Il doit détailler la finalité des cookies et permettre à l'utilisateur d'accepter, refuser ou personnaliser l'acceptation de certains cookies.

## Etape 3 : Recueillir et prouver le consentement éclairé des individus

### 1. Formulaire de collecte de données basé sur le consentement

Formulaire papier ou numérique, vous devez conserver les preuves de consentement des personnes quand votre collecte s'appuie sur cette base légale. On peut réaliser un export sur les outils en ligne de newsletter type Sendinblue/MailChimp *(il faudra créer une fiche d'activité de traitement spécifiquement pour cette conservation de preuve)*

**Le site web permet de créer des bases de données grâce aux « formulaires de contact ». La licéité de toute la base de prospection peut être compromise si le consentement n'est pas conforme. Pour mettre en conformité vos formulaires de contact, il est important de toujours obtenir un consentement actif, éclairé et non-équivoque** ;
- obtenu en opt-in (pas besoin d'un double opt-in !)
- accompagné des informations requises ; finalités de la collecte, nom du responsable de traitement et renvoi à la politique de confidentialité.

**En pratique…**
**Mettez toujours un bouton à activer** ou une case à cocher pour matérialiser le consentement ; « j'accepte de recevoir une offre …. ». Ne précochez-pas vous même !
Placez dessous votre mention d'information.

### 2. Outils newsletter

Pour la newsletter, **configurez vos formulaires pour être conforme** au RGPD, c'est-à-dire indiquez les mentions d'information et mettez en place une case à cocher pour le consentement (opt-in). Envoyer une campagne à toute personne n'ayant pas donné son consentement jusqu'à maintenant.

## Etape 4 : Organiser et justifier le stockage des données

### 1. Procédure de durées de conservation

Le RGPD ne définit pas la durée précise pendant laquelle les données personnelles doivent être conservées : il ne prévoit donc pas de durées spécifiquement « quantifiées ».
En revanche, plusieurs autres textes permettent de définir une durée à appliquer :

- les dispositions légales ou réglementaires de certains textes
- les délibérations de la CNIL : « cadres de référence » de la CNIL
- les références sectorielles (par exemple : code de conduite, etc.)

Si aucune de ces sources ne permet de fixer une durée, il appartient au responsable du traitement de données à caractère personnel, en application du principe général de responsabilité, de **définir cette durée.** Pour cela, il devra **se fonder sur la finalité** pour laquelle le traitement des données personnelles est mis en œuvre, c'est-à-dire le but qu'il poursuit. Il convient donc d'identifier et évaluer ses besoins opérationnels.

### 2. Procédure de stockage des données

Préciser dans cette procédure les **mesures de sécurité mises en œuvre** en fonction du type de données (données de santé notamment) mais aussi les lieux de double sauvegarde.

### 3. Registre des activités de traitement

La constitution du registre vous permet de vous interroger sur les données dont votre entreprise a réellement besoin.

Pour chaque fiche de registre créée, vérifiez que :

- les données que vous traitez sont nécessaires à vos activités
- vous ne traitez aucune donnée dite « sensible » ou, que vous avez bien le droit
- seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- vous ne conservez pas vos données au-delà de ce qui est nécessaire.

Gardez en **archives les différentes mises à jour**, c'est la preuve de votre mise en conformité.

## Etape 5 : Garantir la sécurité des données

### Contrats sous-traitants

Le responsable de traitement doit s'assurer que son sous-traitant respecte le RGPD. Pour ce faire, le contrat doit impérativement **comporter une clause** selon laquelle le sous-traitant tient à disposition du donneur d'ordre toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'article 28 du RGPD.

### Charte informatique

Doit être annexée au règlement intérieur ou les règles qui la composent doivent être mentionnées dans le contrat de travail pour être opposable au salarié.

### Registre des habilitations (arrivée/départ/absence)

Document interne qui définit les habilitations en fonction des fichiers de données, mais aussi de **qui a besoin d'y accéder** en fonction des finalités. (prévoir les absences et départs)

### Politique de sécurité des systèmes d'information (presta informatique/cabinet DPO externe)

Elle se traduit par la réalisation d'un document qui regroupe l'ensemble des règles de sécurité à adopter ainsi que le plan d'actions ayant pour objectif de maintenir le niveau de **sécurité de l'information** dans l'organisme

**Sécurité physique :** Mettre vos archives et documents papier dans un local fermé à clé. La clé doit être accessible aux seules personnes qui en ont besoin.

**Sécurité informatique :**

Pour les authentifications :
- Imposez-vous des mots de passe complexes en les changeant régulièrement
- Pas de stockage en clair de mots de passe, exemple : Keepass
- Accès limités aux seules personnes habilitées.

Pour vos machines :
- Installation et mise à jour régulière de vos antivirus
- stockage des PC de votre structure sous clé
- mot de passe pour allumer le PC !!!
- programmer des sauvegardes régulières de vos données sur serveur ou disque dur externe

### Procédure faille sécurité et notification à la CNIL

**Il y a violation quand on constate une perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite.**

Dans tous les cas, vous devez documenter en interne l'incident en déterminant :
- la nature de la violation
- si possible, les catégories et le nombre approximatif de personnes concernées
- les catégories et le nombre approximatif d'enregistrements de données concernés;
- décrire les conséquences probables de la violation de données ;
- décrire les mesures prises ou que vous envisagez de prendre pour éviter que cet incident se reproduise ou atténuer les éventuelles conséquences négatives.

**Vous devez le notifier à la CNIL dans les meilleurs délais, au plus tard dans les 72 heures, en utilisant le téléservice de notification de violations.**

## Etape 6 : S'organiser en interne pour intégrer le RGPD en amont

### 1. Procédure de Privacy by design

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

### 2. Formations en interne et registre des formations

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

## Etape 7 : Anticiper un contrôle de la CNIL

### 1. Procédure en cas de contrôle CNIL sur place/en ligne/à distance

La conformité d'un organisme au RGPD est une **démarche permanente et dynamique** qui ne doit pas se limiter aux premiers jours de la prise de fonction du DPO.

**Bilan du RGPD 3 ans après**

Malgré les outils de la CNIL et les solutions existantes, 77% des entreprises françaises ne sont pas en conformité avec le RGPD (selon le dernier rapport « Data Risk & Security 2020 »).

***RGPD : Les principales évolutions réglementaires***

4- **Une intensification et simplification des contrôles** : Des contrôles accentués dus à une forte augmentation des plaintes (1000/mois). Des contrôles au contenu très étendu mais avec des problématiques récurrentes qui placent en risque : prospection, durée de conservation, exercice des droits des personnes, responsabilité du fait des partenaires.

5- **Et l'augmentation corrélative des sanctions amendes** : Le nombre et le montant global et individuel d'amende est en très forte augmentation : 51M€ en 2019 et 138M€ en 2020. Les amendes sont adressées à toutes les formes d'acteurs : Associations, Collectivités, Professions libérales, PME/PMI, grands groupes. Un projet de loi doit réaménager les pouvoirs de sanction (un panel plus large de sanctions), simplifier la procédure de mise en demeure et surtout permettre au président de la CNIL de prononcer des sanctions d'un montant maximal de 20 000€ pour les affaires simples et de faible gravité.

*Mettez en conformité votre site internet (porte d'entrée (avec les plaintes) des contrôles).*

*Utiliser un outil tel que la plateforme dédiée aux associations à venir

Récap Etapes :

- *Informer les tiers de l'utilisation de leurs données personnelles*
- *Mettre les outils de prospection en conformité avec le rgpd*
- *Identifier les actions à mener en termes de sécurité informatique*
- *Diffuser à tous le process d'exercice des droits des personnes*