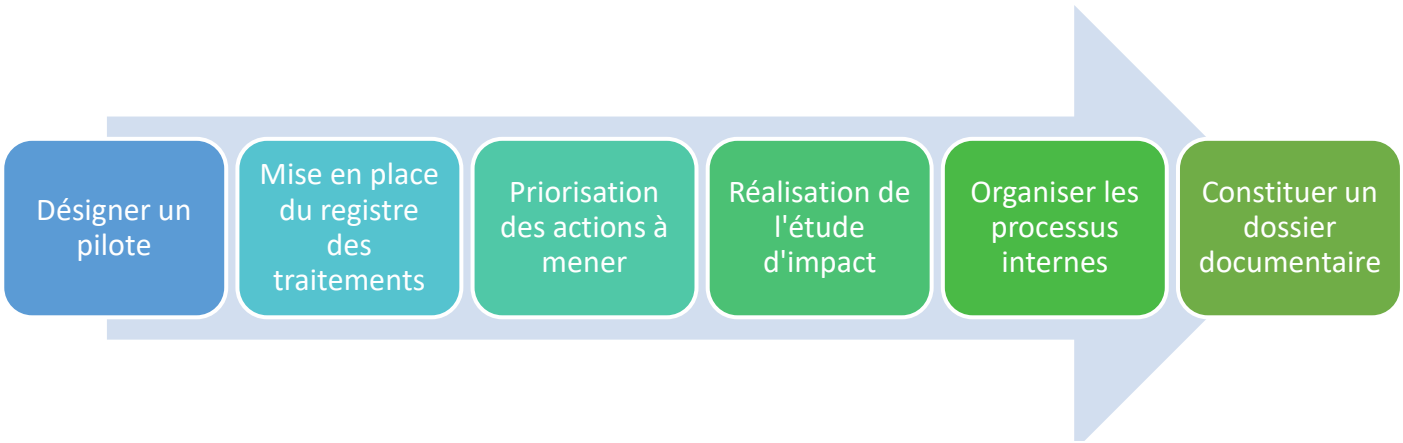
Mise en place du RGPD

Le RGPD est le nouveau règlement européen sur la protection des données.
*Il entrera en application le **25 mai 2018** et impactera toutes les entreprises traitant des données à caractère personnel sur des résidents européens.*

» **Objectif du RGPD** :

- **Uniformiser la réglementation sur la protection des données**.
- **Responsabiliser** davantage les professionnels
- **Renforcer le droit des personnes** (droit à l'accès, droit à l'oubli, droit à la portabilité, etc.).

» **Etapes du RGPD** :



» **Type de données nécessitant une vigilance particulière** :

- Les données sensibles :
  - ✓ Les **origines raciales** ou **ethniques**,
  - ✓ Les **opinions politiques, philosophiques ou religieuses** ou **appartenance syndicale** des personnes,
  - ✓ Les données **biométriques, génétiques** et **liées à la vie sexuelle**
  - ✓ Les données **d'infraction** ou **de condamnation pénale**
  - ✓ Les données **concernant les mineurs**
- Les données de santé :
  - ✓ Données relatives à **la santé physique ou mentale**, passée, présente ou future, d'une personne physique qui révèlent des informations sur son état de santé.
  - ✓ Trois catégories de données de santé :
    - **Données de santé par nature** : antécédents médicaux, maladies, résultats d'examens…
    - **Données du fait de leur croisement avec d'autres données** : croisement de la mesure de la tension avec la mesure de l'effort, croisement d'une mesure de poids avec d'autres données…
    - **Celles qui deviennent des données de santé en raison de leur destination** : c'est-à-dire de leur utilisation qui en est faite sur le plan médical.

1 - Désignation d'un délégué des protections des données (=DPO) ou d'un Correspondant Informatique & Liberté

Véritable chef d'orchestre pour piloter la conformité et la gouvernance des données personnelles de la structure, il exerce une mission d'information, de conseil et de contrôle en interne.

» La **désignation d'un DPO** est obligatoire pour :
- Les **organismes ou autorités publics**
- Les **organisations dont l'activité de base l'amène à réaliser un suivi régulier et systématique des personnes à grande échelle** (ex. banque, compagnie d'assurances...)
- Les **organisations traitant des données sensibles** (ex. hôpital, laboratoire.)

Cette désignation implique nécessairement d'en informer l'autorité compétente : la CNIL en France (https://www.cnil.fr/fr/designation-dpo)

» Vérifier que le DPO dispose du **statut, des compétences et des moyens nécessaires à l'exercice de ses missions** :
- *Capacité d'agir en toute indépendance*
- *Compétences requises* :
  - ✓ **Connaissances juridiques et techniques** en matière de protection des données personnelles nécessaires à l'accomplissement de ses missions ;
  - ✓ **Bonne connaissance du secteur d'activité et de l'organisation interne de l'organisme**, en particulier **des opérations de traitements, des systèmes d'informations, des besoins en matière de protection et de sécurité des données**.
- Moyens nécessaires :
  - ✓ Disposer **du temps suffisant** pour exercer sa mission ;
  - ✓ Bénéficier **des moyens matériels** et **humains adéquats** ;
  - ✓ Avoir accès aux **informations utiles** ;
  - ✓ Être associé en amont des projets impliquant des données personnelles

» Le **rôle du DPO** :
- **Informer et conseiller** le responsable de traitement ou le sous-traitant ainsi que les employés
- **Contrôler le respect du règlement et du droit national** en matière de protection des données
- **Conseiller l'organisation sur la réalisation d'études d'impact** sur la protection des données et d'en vérifier l'exécution
- **Coopérer avec l'autorité de contrôle** et d'être le *point de contact* avec celle-ci

» **Missions du DPO** :
- **Informer** sur le contenu des nouvelles obligations
- **Sensibiliser les décideurs** sur l'impact de ces nouvelles règles
- **Réaliser l'inventaire des traitements de donnés** de votre organisme
- **Concevoir des actions** de sensibilisation
- **Piloter la conformité** en continu

2 – Mise en place d'un registre des traitements

*Les organisations **doivent tenir une documentation interne complète sur leur traitement de données personnelles** et s'assurer que ces traitements respectent bien les nouvelles obligations légales. L'objectif est d'avoir une vision d'ensemble claire de tous les traitements de données personnelles effectués par le responsable du traitement.*

» Le **registre est obligatoire** pour tous les responsables de traitement si :
- Les **organisations d'au moins 250 salariés**
- Les **organisations qui effectuent des traitements de données sensibles**

» **Conditions d'établissement** du registre :
- Registre doit être **nécessairement sous forme écrite**, même s'il est réalisé électroniquement
- Registre doit être **mis à disposition de l'autorité de contrôle** (CNIL)

» Afin d'être en capacité de mesurer l'impact du règlement sur l'activité de l'organisation et de répondre à l'exigence de registre il est nécessaire de **recenser au préalable** :
- Les **différents traitements** de données personnelles
- Les **catégories de données personnelles traitées**
- Les **objectifs poursuivis** par les opérations de traitement de données
- Les **acteurs**, internes et/ou externes, qui traitent ces données dont les prestataires sous-traitants
- Les **flux**, avec l'origine et la destination des donnés afin d'identifier les éventuels transferts de données à l'étranger

» **Mentions obligatoires à faire figurer** dans le registre :
- **Nom et coordonnées du responsable** de traitement, de son responsable légal et du DPO ;
- **Finalités** du traitement
- **Catégories de personnes et données concernées ; destinataires éventuels des données** ;
- **Transfert** éventuellement prévu vers un pays tiers
- **Délais d'effacement** prévus par type de données
- Description globale **des mesures techniques et organisationnelles prises pour assurer la sécurité des données**

Modèle de registre : REGISTRE DES TRAITEMENTS.rtf

3 – <u>Priorisation les actions à mener</u>

Après avoir identifié les traitements de données personnelles mis en œuvre au sein de l'organisation, il faut identifier les actions à mener pour se conformer aux nouvelles obligations ***et prioriser les actions au regard des risques que font peser les traitements sur les droits et libertés des personnes concernées***.

Quels que soient les traitements de données :

- **S'assurer que seules les données strictement nécessaires à la poursuite des objectifs sont collectées et traitées**
- **Identifier la base juridique** sur laquelle se fonde le traitement
- **Réviser les mentions d'information**
- **Vérifier que les sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités** (clauses contractuelles doivent rappeler les obligations du sous-traitant en matière de sécurité, confidentialité et protection des données traitées)
- **Prévoir les modalités d'exercice** des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...)
- **Vérifier les mesures de sécurité** mises en place
- **Identifier les traitements à risques**

4 – Réalisation d'une étude d'impact

*Une **étude d'impact sur la protection des données** doit être effectuée avant de collecter des données et pour chacun des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées.*

Il s'agit donc d'**identifier les risques afin de déterminer les mesures proportionnées** :

- **Les éléments à protéger** : minimiser les données, chiffrer, anonymiser, permettre l'exercice des droits…
- **Les impacts potentiels** : sauvegarder les données, tracer l'activité, gérer les violations de données…
- **Les sources de risques** : contrôler les accès, gérer les tiers, lutter contre les codes malveillants…
- **Les supports** : réduire les vulnérabilités des matériels, logiciels, réseaux, documents papier

» **L'étude d'impact permet** :

- **De bâtir un traitement de données personnelles ou un produit respectueux de la vie privée**
- D'apprécier **les impacts sur la vie privée** des personnes concernées
- De **démontrer que les principes fondamentaux du règlement sont respectés**

» **L'étude d'impact doit contenir** :

- Une **description du traitement** et de **ses finalités**
- Une **évaluation de la nécessité et de la proportionnalité du traitement**
- Une **appréciation des risques sur les droits et libertés des personnes concernées**
- Les **mesures envisagées pour traiter les risques** et se conformer au règlement

L'étude d'impact peut s'effectuer sur l'outil PIA qui s'adresse principalement aux responsables de traitement n'étant pas ou étant peu familiers avec la démarche. Il s'agit d'une **version « prêt à l'emploi ». Téléchargez et installez le lien ici : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil**

Des outils sont mis à disposition sur la CNIL pour aider le responsable des traitements à **déterminer les mesures proportionnées aux risques identifies.**

Exemple de tableau d'étude d'impact :

Risques	Impacts sur les personnes	Principales sources de risques	Principale menaces	Mesures existantes ou prévues	Gravite	Vraisemblance
Accès illégitime à des données						
Modification non désirée de données						
Disparition de données						

5 – Organiser les processus internes

Les procédures internes doivent ***garantir un haut niveau de protection des données personnelles en permanence en prenant en compte l'ensemble des évènements qui peuvent survenir au cours de la vie d'un traitement de données*** *: faille de sécurité, modification des données collectées, changement de prestataire etc.*

» **L'organisation des processus internes passe par** :

- **Prendre en compte la protection des données personnelles** dès la conception d'une application ou d'un traitement
- **Sensibiliser et organiser la remontée d'information** en construisant notamment un plan de formation et de communication auprès des collaborateurs
- **Traiter les réclamations et les demandes** des personnes concernées quant à l'exercice de leurs doits en définissant et les acteurs et modalités
- **Anticiper les violations de données** en prévoyant la *notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais*.
- **Mises à jour fréquentes des procédures**
- **Rédiger une charte informatique** en annexe au règlement intérieur :
  - ✓ Rappel des règles et des sanctions sur la protection des données
  - ✓ Le champ d'application de la charte qui inclut : les modalités d'intervention, les moyens d'authentification utilisés par l'organisme et les règles de sécurité
  - ✓ Les modalités d'utilisation des moyens informatique et de télécommunication mis à disposition.
  - ✓ Les conditions d'administration du système d'information
  - ✓ Les responsabilités et sanctions encourus en cas de non-respect de cette charte

6 – Constituer un dossier documentaire

Les organisations ***doivent constituer et regrouper la documentation nécessaire permettant de démontrer que le traitement des données personnelles est conforme au règlement européen****.*
Pour cela les mesures organisationnelles et techniques devront être réexaminées et actualisées en fonction des évolutions.

» **Le dossier documentaire doit comporter** :

- **La documentation sur le traitement des données personnelles** ;
  - ✓ Le registre des traitements ou des catégories d'activité de traitements pour les sous-traitants
  - ✓ Les analyses d'impact
  - ✓ L'encadrement des transferts de données à l'étranger
- **L'information des personnes** ;
  - ✓ Les mentions d'information
  - ✓ Les modèles de recueil des consentements des personnes concernées
  - ✓ Les procédures mises en place pour l'exercice des droits des personnes
- **Les contrats qui définissent les rôles et les responsabilités des acteurs**
  - ✓ Les contrats avec les sous-traitants
  - ✓ Les procédures internes en cas de violations des données
  - ✓ Les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base

7 - Sanctions

*L'article 83 du RGPD stipule que des **sanctions effectives, proportionnées et dissuasives** seront délivrées pour toute violation du RGPD.*

» **Montants des amendes :**

- Les amendes peuvent s'élever à **20 000 000 €** ou à **4%** du chiffre d'affaires mondial
- Le montant des amendes est variable selon :
  - ✓ La **nature, la gravité et la durée de la violation**
  - ✓ La **portée** ou la **finalité du traitement** concerné
  - ✓ Le **nombre de personnes affectées** et le **niveau de dommage** qu'elles ont subi.
  - ✓ Le **degré de responsabilité** du responsable de traitement ou du sous-traitant
  - ✓ Les **différentes mesures techniques** et **organisationnelles** déjà mises en place pour assurer la conformité de la société.

» **Responsabilité du responsable ou du sous-traitant**

- Si un responsable du traitement ou un sous-traitant **viole délibérément ou par négligence** plusieurs dispositions du présent règlement, **le montant total de l'amende administrative ne peut pas excéder le montant fixé** pour la violation la plus grave.