CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

NEC ORLÉANS

LES BONNES PRATIQUES EN MATIERE DE DONNEES PERSONNELLES

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

- PRÉSENTATION DE LA CNIL
- PRINCIPES GÉNÉRAUX
- CAS PRATIQUES
- RÉPONSES AUX QUESTIONS

CONTEXTE HISTORIQUE

CNIL
Commission Nationale de l'Informatique et des Libertés

CNIL
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Années 70

Augmentation de la **création de fichiers informatiques et de bases de données**.

Naissance de nouveaux débats.

21 mars 1974

Projet SAFARI :

Le Gouvernement souhaite créer une base de données de la population française et utiliser le **numéro de sécurité sociale** comme identifiant.

6 janvier 1978

Face au scandale**, le projet est annulé.**

Naissance de la **CNIL** et de la **Loi Informatique et Liberté** (LIL).

27 avril 2016

Création du **Règlement général sur la protection des données personnelles** (RGPD).

25 mai 2018

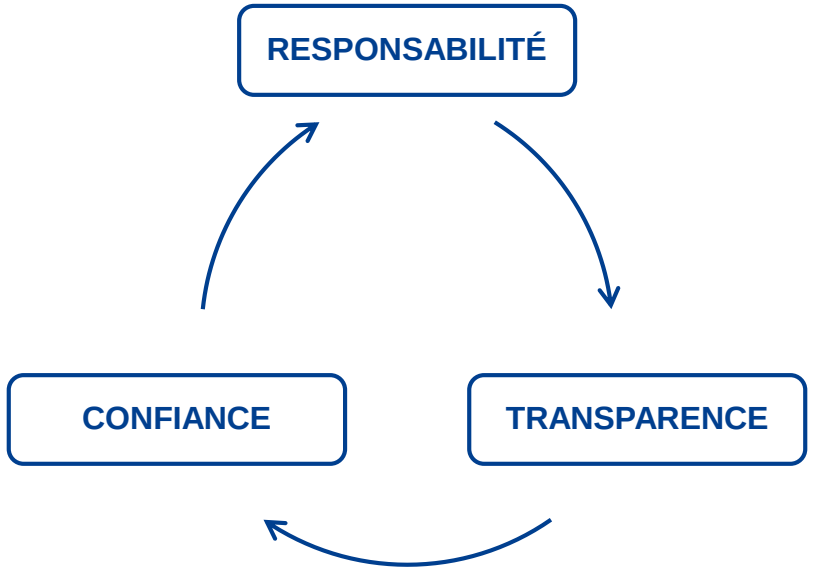
Entrée en application du RGPD.

LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD)

Entré en application le 25 mai 2018

Il a permis de :

- **Renforcer les droits** des personnes
- **Responsabiliser** les acteurs des données
- **Renforcer** les pouvoirs de sanctions
- Faire **disparaître** la majorité des **formalités** (déclarations, autorisations)



Qui est concerné ?

Toute organisation, **publique ou privée**, qui traite **des données personnelles**, pour son compte ou non, dès lors qu'elle :

- **Qu'elle est établie sur le territoire de l'UE;**
- **Que son activité cible directement des résidents européens.**

LES MISSIONS DE LA CNIL

INFORMER ET PROTÉGER LES DROITS

ACCOMPAGNER LA CONFORMITÉ

ANTICIPER ET INNOVER

CONTRÔLER ET SANCTIONNER

LES PRINCIPALES NOTIONS

DONNÉES PERSONNELLES
DONNÉES SENSIBLES

TRAITEMENT DE DONNÉES PERSONNELLES

RESPONSABLE DE TRAITEMENT ET SOUS-TRAITANT

DÉLÉGUÉ À LA PROTECTION DES DONNÉES

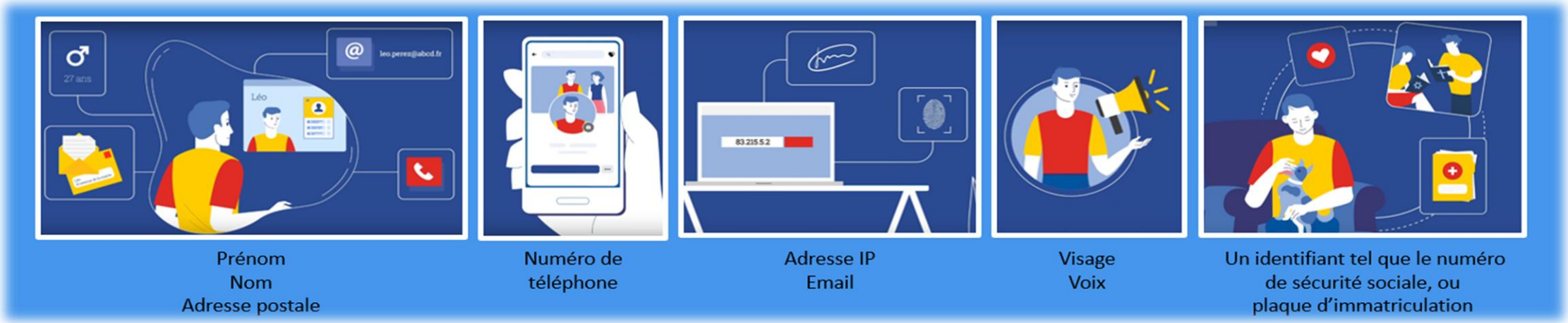
CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PRINCIPES GENERAUX

QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

Toute information relative à une personne physique identifiée ou identifiable

Une personne peut être identifiée :
- **Directement** (nom, prénom, …)
- **Indirectement** (n° de client, de téléphone, voix, image, …)



QU'EST-CE QU'UNE DONNÉE SENSIBLE ?

En principe, il est **interdit** de collecter ou traiter ces données, *sauf exceptions*.

Les données sensibles sont celles qui concernent :

- La prétendue **origine raciale ou ethnique**
- Les **opinions politiques**
- Les **convictions religieuses** ou **philosophiques** ou **l'appartenance syndicale**
- Les données **génétiques** et **biométriques**
- Les données de **santé**
- Les données concernant la **vie sexuelle** ou **l'orientation sexuelle**

Handicap, donnée sensible ?
La notion de « handicap » sera considérée comme sensible si elle permet d'établir la nature du handicap ou une pathologie

Les données relatives :

- aux **condamnations pénales**
- aux **infractions**
- aux **mesures de sûretés**

→ ne peuvent être collectées *que dans les cas précisés par l'article 46 de la LIL*

Le numéro de sécurité sociale (NIR)

→ l'utilisation doit être *prévue dans le décret NIR*

LES EXCEPTIONS

LE RGPD, *article 9.2* établit une liste de cas dans lesquels il est **autorisé** de collecter et traiter des données sensibles :

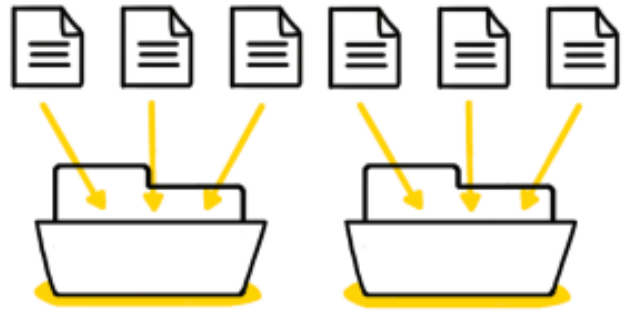
QU'EST-CE QU'UN TRAITEMENT ?

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles :

- Collecte
- Enregistrement
- Organisation
- Conservation
- Adaptation
- Modification
- Extraction
- Consultation
- Utilisation
- Communication par transmission, diffusion ou toute autre forme de mise à disposition
- Rapprochement

Exemple : *Tenue d'un fichier de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, etc.*

La réglementation s'applique également sur les **fichiers papier.**



RESPONSABLE DE TRAITEMENT (RT)

La **personne**, **l'autorité publique**, la **société** ou **l'organisme** qui :

- **Détermine les finalités et les moyens** du fichier
- Qui **décide de sa création**

En pratique, il s'agit de la personne morale (entreprise, collectivité, etc.) incarnée par son représentant légal (président, maire, etc.)

Plusieurs organismes peuvent être « **co-responsables de traitement** »

SOUS-TRAITANT (ST)

La **personne physique ou morale** (entreprise ou organisme public) qui :

- **Traite des données pour le compte d'un autre organisme** (le responsable de traitement)
- Agit **sur instruction** du RT

Dans le cadre d'un **service ou d'une prestation**.

La relation RT-ST doit **obligatoirement** être encadrée par un **contrat de sous-traitance**

DPO / DPD

Le Délégué à la Protection des données
Data Protection Officer

« **chef d'orchestre** » de la conformité en matière de protection des données au sein d'un organisme

La désignation d'un délégué est **obligatoire** pour :

- Les **autorités ou les organismes publics**
- Les organismes dont les activités les amènent à réaliser un **suivi régulier et systématique des personnes à grande échelle**
- Les organismes dont les activités les amènent à **traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions**

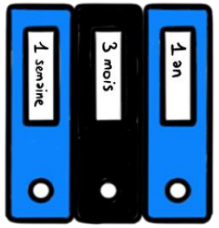
*En dehors de ces cas, la désignation d'un DPO est **recommandée** mais n'est pas obligatoire.*

Le DPO n'est **pas personnellement responsable** en cas de **manquement** au RGPD.

➡ **C'est l'organisme qui est responsable.**

Délégué à la protection des données

LES GRANDS PRINCIPES

	1. Finalité du traitement
	2. Principe de minimisation et de pertinence
	3. Base légale
	4. Durée de conservation limitée

	4. Transparence et information
	6. Sécurité des données
	7. Droits des personnes

LA FINALITÉ

La finalité du traitement est l'objectif principal de l'utilisation des données personnelles

La **finalité** doit :

- ❑ Être **déterminée**, **légitime** et **explicite**
- ❑ Être **respectée**
- ❑ Respecter le **principe de minimisation** et de **pertinence**

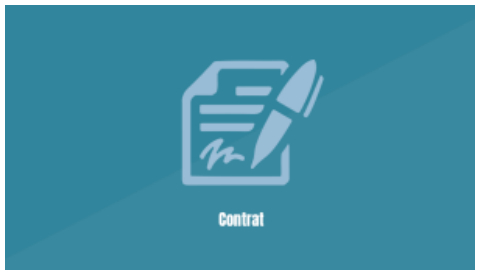
Exemple de finalité :

- Gestion des recrutements
- Gestion de la paie
- Gestion des clients
- Enquête de satisfaction
- Surveillance des locaux, etc.

LA BASE LÉGALE

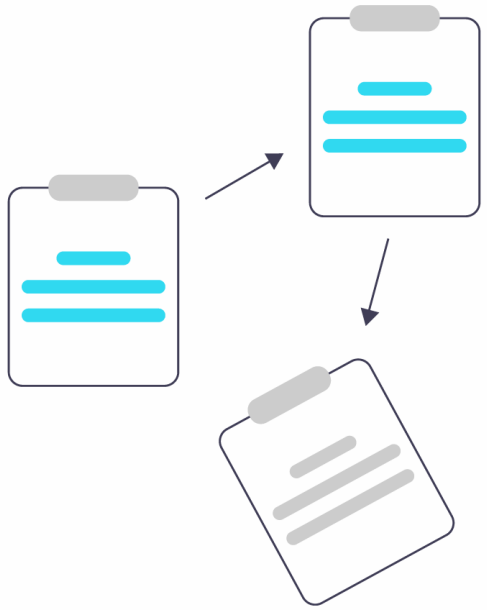
La base légale d'un traitement est ce qui autorise légalement sa mise en œuvre

1. Le **consentement** : La personne a consenti au traitement de ses données
2. Le **contrat** : Le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée
3. L'**obligation légale** : Le traitement est imposé par des textes légaux
4. La **mission d'intérêt public** : Le traitement est nécessaire à l'exécution d'une mission d'intérêt public
5. L'**intérêt légitime** : Le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données dans le respect des droits et intérêts des personnes dont les données sont traitées
6. La **sauvegarde des intérêts vitaux** : Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers



LA CONSERVATION DES DONNÉES

Une durée de conservation précise des données doit être fixée en fonction de chaque finalité



La **durée de conservation** est fixée par le responsable de traitement :

- ❑ Elle peut être prévue par un **texte légal**
- ❑ Elle peut être recommandée par la **CNIL**
- ❑ Elle peut être fixée **au regard de la finalité**

Pas de conservation indéfinie ni de conservation « au cas où » des données.

L'INFORMATION DES PERSONNES

Lorsque vous collectez des données, vous devez fournir les informations suivantes :

- **Identité et coordonnées de l'organisme** (responsable du traitement de données)
- **Finalités** (à quoi vont servir les données collectées)
- **Base légale** du traitement de données
- **Caractère obligatoire ou facultatif du recueil des données**
- **Destinataires ou catégories de destinataires des données**
- **Durée de conservation des données** (ou critères permettant de la déterminer)
- **Droits des personnes concernées**
- **Coordonnées du délégué à la protection des données**
- **Droit d'introduire une réclamation auprès de la CNIL**

Des exemples de mentions d'informations sont disponibles sur le site de la CNIL

SÉCURISER LES DONNÉES

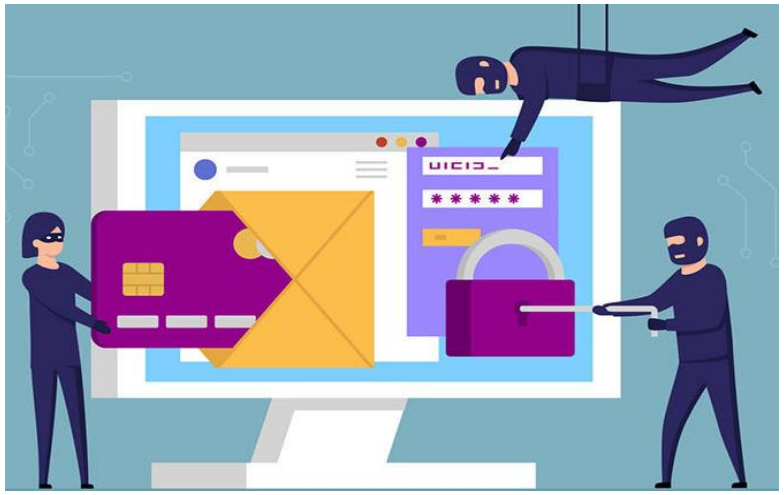
Le responsable de traitement assure la sécurité des données personnelles

Le responsable d'un fichier doit **prendre les précautions utiles** pour assurer la sécurité des données et **empêcher que des tiers non autorisés y aient accès.**

- ✓ Mettre à jour de vos antivirus et logiciels,
- ✓ Utiliser des mots de passe complexes,
- ✓ Utiliser des gestionnaires de mots de passe,
- ✓ Effectuer des sauvegardes régulières,
- ✓ Sécuriser l'accès Wi-Fi, protéger les données lors de déplacements,
- ✓ Être prudent en utilisant des messageries,
- ✓ Séparer les usages personnels des usages professionnels, etc.

Que faire en cas de **violation de données personnelles** ?

- ➢ **Documenter** les violations en interne
- ➢ **Notifier à la CNIL, dans les 72h,** celles qui présentent un risque pour les droits et libertés des personnes
- ➢ Prévenir les personnes concernées **en cas de risque élevé**



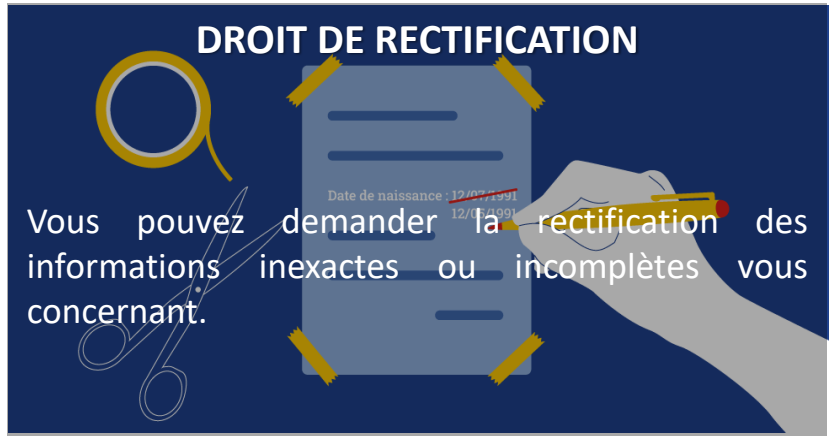
LES DROITS DES PERSONNES

DROIT D'ACCÈS

Vous pouvez demander à un organisme :

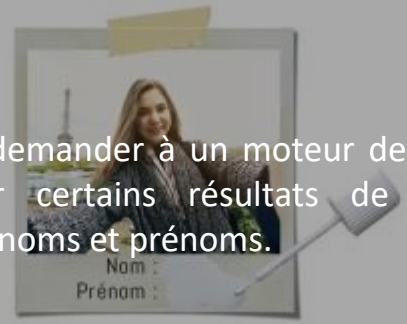
- S'il détient des données sur vous
- De vous communiquer les données vous concernant pour en vérifier le contenu

DROIT DE RECTIFICATION



Vous pouvez demander la rectification des informations inexactes ou incomplètes vous concernant.

DROIT AU DÉRÉFÉRENCEMENT

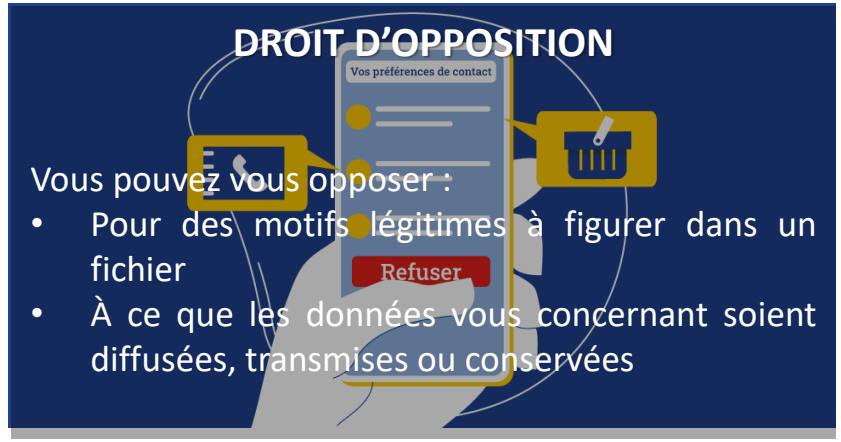


Vous pouvez demander à un moteur de recherche de supprimer certains résultats de recherche associés à vos noms et prénoms.

DROIT À LA PORTABILITE

Vous pouvez récupérer une partie de vos données dans un format lisible par une machine. Libre à vous de les stocker ailleurs ou de les transmettre d'un service à un autre.

DROIT D'OPPOSITION



Vous pouvez vous opposer :

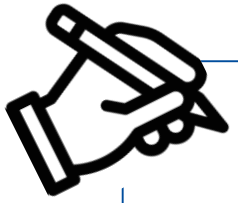
- Pour des motifs légitimes à figurer dans un fichier
- À ce que les données vous concernant soient diffusées, transmises ou conservées

DROIT À L'EFFACEMENT

Vous avez le droit de demander à un organisme l'effacement des données vous concernant.

EXERCICE DES DROITS

Vous devez permettre aux personnes d'exercer facilement leurs droits



Ces droits peuvent être exercés :

- Par voie électronique (formulaire, courriel, etc.)
- Par courrier postal

Délai à respecter :

Vous disposez de **1 mois** pour répondre à la demande

➡ En cas de **demande complexe** : ce délai peut être **prolongé de 2 mois**

(**MAIS** vous devez en informer la personne dans le délai de 1 mois)

- Si la personne n'a **pas obtenu de réponse** dans le délai ou n'a **pas obtenu une réponse satisfaisante** : **elle pourra saisir la CNIL d'une plainte**
- Tout individu peut exercer ses droits par **l'intermédiaire d'une personne ou d'un organisme mandaté**. La CNIL a publié sur son site un **MANDAT-TYPE**

LE REGISTRE

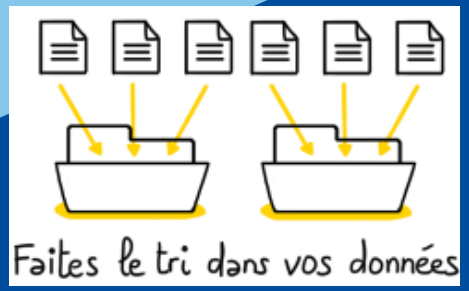
La CNIL a publié un modèle de registre et son propre registre des activités de traitement

- ✓ **Recenser les traitements de données** et avoir une vue d'ensemble des données personnelles
- ✓ **Pour tous les organismes**, publics, privés et quelle que soit leur taille, **dès lors qu'ils traitent des données personnelles**
- ✓ **Forme écrite libre** au format papier ou électronique
- ✓ Doit contenir **une fiche par activité de traitement** (exemple : gestion de la paie, vente en ligne, etc.)

  - ❑ Le **nom et les coordonnées** de l'organisme et du DPO
  - ❑ Les **finalités** du traitement
  - ❑ Les **catégories de personnes concernées** (client, prospect, employé, etc.)
  - ❑ Les **catégories de données personnelles** (exemples : identité, situation familiale, données bancaires, etc.)
  - ❑ Les **catégories de destinataires** (sous-traitant, partenaire commercial, etc.)
  - ❑ Les **transferts de données** à caractère personnel vers un pays tiers ou à une organisation internationale
  - ❑ Les **délais de conservation**
  - ❑ Les **mesures de sécurité**

RÉSUMÉ

- ❑ **RECENSER LES FICHIERS**
- ❑ **FAITES LE TRI DANS LES DONNÉES**
- ❑ **FAITES PREUVE DE TRANSPARENCE**
- ❑ **ORGANISEZ ET FACILITEZ L'EXERCICE DES DROITS DES PERSONNES**
- ❑ **SÉCURISER LES DONNÉES**



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

FOCUS SECTEUR SOCIAL

QUAND JE FORME

Je l'informe	• Si les actions que l'usager effectue sur un poste public son enregistrées, si son écran est déporté sur le mien, etc.
Je sensibilise	• Je l'oriente vers des outils respectueux de la vie privée ou la navigation privée. Je lui explique les bonnes pratiques en matière de protection des données.
Je demande le moins d'informations possible	• Je ne collecte pas de données inutilement, je n'enregistre pas automatiquement les informations dans le navigateur, je privilégie des données fictives.
Je l'incite à effacer ses traces	• J'efface l'historique de navigation, j'incite à refuser les cookies, je vérifie sur l'usager est bien déconnecté de sa session.
J'évite les fuites	• Si j'envoie un courriel groupé, je pense à cacher les adresses (Cci).

QUAND J'ACCOMPAGNE

EN SA PRÉSENCE

Je reste discret	• En tant qu'accompagnateur je suis soumis à une obligation de confidentialité, notamment envers les informations fournies par l'usager (vie personnelle, identifiants de connexion, etc.).
Je ne conserve pas ses informations	• Je ne conserve pas les informations de l'usager à la fin de la session, et notamment ses identifiants et mots de passe.
J'informe en toute transparence	• J'informe l'usager de mon rôle et j'évoque avec lui des bonnes pratiques pour limiter ses traces, exercer ses droits Informatique et Libertés, etc.
Je reste vigilant sur les traces	• J'incite l'usager à refuser le dépôt de cookies et à utiliser une navigation privée. • Je vérifie que l'usager s'est bien déconnecté de sa session une fois les démarches réalisées et qu'il a supprimé les éventuelles documents téléchargés sur le poste.

❑ Je demande son accord (mandat écrit)

Pour garantir la **validité du mandat**, vous devez expliquer à l'usager :

- **l'objet** de votre intervention ;
- la **raison** pour laquelle ses informations sont collectées ;
- la possibilité pour l'usager de **révoquer à tout moment** le mandat.

La CNIL propose un modèle de mandat sur son site.

❑ Le mandat oral

Lorsqu'il est impossible de recueillir le consentement de l'usager, un **mandat pourra être donné oralement**.

- procéder à un « **contrôle d'identité** » plus ou moins poussé au regard du risque potentiel pour la personne concernée, et des possibilités dont disposent les agents traitant les demandes ;
- **tracer en interne chaque demande** de façon nominative et horodatée ;
- adresser le plus rapidement possible une **confirmation écrite de la démarche réalisée** ;
- **informer** la personne concernée de la possibilité de **révoquer à tout moment son mandat**.

❑ Je fais preuve de transparence

- Je ne **collecte et n'utilise que les données nécessaires** à la tâche prévue dans le mandat.
- Je **ne conserve pas inutilement** les données.
- Si l'usager n'a pas d'adresse courriel je lui propose de lui en **créer une pour les démarches administrative** dans le cadre du **mandat**.

❑ Je veille à la confidentialité de ses données

- Je **n'enregistre pas dans le navigateur** les mots de passe de l'usager.
- Si le mandat le prévoit, seules **deux techniques permettent de conserver ses mots de passe** : un gestionnaire de mots de passe ou un carnet stocké dans un coffre-fort.
- Je **déconnecte l'usager** de tous ses comptes.
- Un collègue de travail peut avoir accès aux données **en cas de nécessité**, par exemple pour assurer la continuité d'un accompagnement en cas de congés et à la condition d'une part, d'en informer la personne concernée et d'autre part, d'obtenir son accord.

FOCUS : Le mot de passe

Ne demander la communication des identifiants et mots de passe de l'espace personnel d'un usager que si celui-ci n'est pas en capacité de se connecter seul. Il doit s'agir de situations exceptionnelles.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

CAS PRATIQUES

MISE EN PRATIQUE

**Afin d'accompagner un usager dans ses démarches,
dans quels cas puis-je demander ses identifiants et ses mots de passe ?**

1. S'il n'a pas d'accès à Internet ✓

2. S'il n'est pas en mesure de se déplacer ✓

3. S'il n'est pas en capacité de se connecter seul ✓

4. Si je souhaite effectuer ses démarches sans mandat ✗

MISE EN PRATIQUE

Comment conserver leurs identifiants et leurs mots de passe ?

1. Gestionnaire de mots de passe (Keypass)

2. Carnet stocké dans un coffre- fort

3. Sur un post-it

4. Carnet dans un tiroir non verrouillé

MISE EN PRATIQUE

Est-ce un bon mot de passe ?

1. Azerty

2. 1234

3. 0000

4. Nomprénomdatedenaissance

5. Hgfjghl^pjkuipo28!fhui(g)

6. 1mô2passeFacileàmesouvenir!

MISE EN PRATIQUE

Quelles données puis-je collecter et conserver pour identifier une personne ?

1. Données d'identification :

- Nom, prénom, adresse, date de naissance, etc.
- Photo

2. Nationalité, régularité du séjour en France :

- « français / UE / hors UE »
- « dépôt de demande d'asile : oui / non »
- « dépôt d'une demande de titre de séjour : oui / non »

3. Numéro d'identification de rattachement à un organisme :

- CAF, France Travail, etc.

4. Photocopie pièce d'identité :

Par exemple pour le dépôt d'un dossier de surendettement auprès de la Banque de France.

5. Numéro de sécurité sociale (NIR) :

Dans les cas prévus par le décret n°2019-341, 19 avril 2019.

MISE EN SITUATION

Madame Y souhaite postuler à une offre d'emploi en ligne mais n'a pas d'accès à internet et ne maîtrise pas bien l'informatique.

Elle souhaite donc être accompagnée dans sa démarche.

Quels sont les bons réflexes pour protéger ses données personnelles ?

- ❑ Ne transmettre **que les données nécessaires** à l'analyse de la candidature au poste.
- ❑ Ne **pas transmettre :**
  - le NIR,
  - les informations relatives aux membres de la famille,
  - les anciens bulletins de paie,
  - etc.

Pour plus d'informations, consulter le :
Guide de la CNIL sur le RECRUTEMENT.

MISE EN SITUATION

Monsieur X a fait l'objet d'une condamnation pour un délit il y a 15 ans. Lors des faits, le journal local a publié un article en ligne sur cette affaire.

Depuis, lorsque l'on recherche son nom et prénom dans un moteur de recherche, l'article de presse apparaît dans les premiers résultats. Que faire ?

- ❑ Droit **d'opposition**
- ❑ Droit au **déréférencement**
- ❑ Informer que vous pouvez exercer ses droits **à sa place** avec la signature d'un **mandat** (*modèles disponibles sur le site de la CNIL*).

MISE EN SITUATION

Madame X est inquiète, elle vient de recevoir un message de France Travail lui indiquant que ses données ont fait l'objet d'une violation de données personnelles.

Quels sont les bons conseils à lui fournir ?

- ❑ Consulter le **site de la CNIL**
- ❑ Conseiller d'être **vigilant** au risque d'hameçonnage (*phishing*)
- ❑ Vérifier périodiquement les **mouvements sur ses comptes bancaires**
- ❑ Consulter le site **cybermalveillance.gouv.fr**
- ❑ Vérifier que ses **mots de passe sont assez robustes**
- ❑ **Contacter l'organisme concerné** pour plus d'informations

MISE EN SITUATION

Monsieur X reçoit régulièrement de la publicité par courriel de la société Jardiworld.com.

N'étant pas amateur de jardinage, il ne souhaite plus recevoir ce type de sollicitation et se demande comment cette société a pu obtenir son adresse. Que faire ?

- ❑ Exercer son **droit d'accès** pour connaître l'origine de ces données
- ❑ S'**opposer** à la réception ultérieure de prospection commerciale de la part de Jardiworld.com
- ❑ Monsieur X n'a **pas besoin de justifier** sa demande
- ❑ Le courriel de prospection doit normalement lui permettre de se **désabonner facilement**
- ❑ À défaut, il faudra **saisir le DPO** de la société
- ❑ En cas de refus, **saisir la CNIL** d'une plainte

RESSOURCES ET INFORMATIONS UTILES

- **PERMANENCES TÉLÉPHONIQUES : 01 53 73 22 22**
  - **Juridique et DPO** – lundi, mardi, jeudi, vendredi de 10h à 12h
  - **Santé** – lundi de 9h30 à 12h
  - **International** – mercredi de 14h à 16h

- **GUIDES ET REFERENTIELS DE LA CNIL :**