Commission Nationale de l'Informatique et des Libertés

La protection des données personnelles dans la sphère sociale et médico-sociale

Statut et composition de la Cnil

- Une autorité administrative indépendante composée de 17 Commissaires (hauts magistrats, parlementaires, conseillers économiques et sociaux, personnalités qualifiées)

- Un président élu par ses pairs

  Mme Isabelle FALQUE-PIERROTIN, Présidente de la CNIL depuis 2011

- Les membres de la CNIL ne reçoivent d'instruction d'aucune autorité

- Des services : 178 agents contractuels de l'Etat répartis en 5 directions

Les missions de la CNIL

La CNIL veille à l'application de la loi du 6 janvier 1978 également appelée loi « Informatique et Libertés »

- **Réglementer, informer et conseiller** (administrations, entreprises, citoyens)
- **Contrôler** les fichiers a priori et a posteriori
  - ✓ Instruction des dossiers de formalités préalables
  - ✓ Instruction des plaintes
  - ✓ Contrôles sur place, sur pièces ou en ligne
- **Sanctionner** en cas de mise en demeure infructueuse

(sanction pécuniaire, retrait d'autorisation, injonction de cesser le traitement, dénonciation au Procureur)

Trois « notions clefs »

- ✓ **Donnée à caractère personnel**
- ✓ **Traitement de données**
- ✓ **Responsable de traitement**

Qu’est-ce qu’une donnée à caractère personnel (DCP) ?

Toute information relative à **une personne physique identifiée ou qui peut être identifiée, directement ou indirectement**, par référence à un numéro d’identification ou à un ou plusieurs éléments qui lui sont propres

NUMÉRO DE SÉCURITÉ SOCIALE

ADRESSE IP

ADRESSE EMAIL

IDENTIFIANT UNIQUE DE COOKIE

N° DE TÉLÉPHONE

NUMÉRO DE CB

N° CLIENT

NOM, PRÉNOM,
DATE DE NAISSANCE

ADRESSE POSTALE

MATRICULE

Traitement de données à caractère personnel et fichier

✓ **Traitement** :

Toute opération ou ensemble d'opération portant sur une DCP, quel que soit le procédé utilisé (automatisé ou non), notamment la collecte, l'enregistrement, l'organisation, la conservation, la modification, l'extraction, la consultation, l'utilisation, la communication, le rapprochement, l'interconnexion, le verrouillage, l'effacement ou la destruction.

✓ **Fichier** :

Tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés (Ex. : fichier du personnel, fichier des inscriptions scolaires, fichier des aides sociales, fichier des clients et prospects, …)

Le responsable de traitement

✓ **Critères de détermination :**

Le responsable d'un traitement de DCP est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives au traitement, la personne, l'autorité publique, le service ou l'organisme qui **détermine ses finalités et ses moyens**.

En principe le représentant légal de l'organisme : ministre, président directeur, gérant de la collectivité locale, de l'établissement d'enseignement supérieur, de l'organisme de recherche ou de la structure privée concerné(e), etc.

Les règles à respecter

1. Une **finalité** déterminée, explicite et légitime
2. Des **données** adéquates, pertinentes, non excessives et mises à jour
3. Une **durée de conservation** limitée : la consécration d'un « droit à l'oubli »
4. Le respect des **droits des personnes**
5. Des **mesures de sécurité** adaptées : confidentialité, intégrité et pérennité des données

1. Le principe de finalité

Elle doit être **déterminée**, **explicite** et **légitime**

- ✓ Le caractère légitime d'un traitement dépend notamment des missions du responsable de traitement

Exemple : gestion des dossiers des personnes faisant l'objet d'un accompagnement social et/ou médico-social

- ✓ Un fichier ne doit pas servir à d'autres fins que celles pour lesquelles il a été constitué

- ✓ Le détournement de finalité est sanctionné pénalement

2. Le principe de proportionnalité des données …(1/3)

- ✓ La collecte doit être loyale et licite
- ✓ Des données **adéquates**, **pertinentes** et **non excessives** par rapport à la finalité poursuivie

→ Obligation de « minimiser » les données traitées

- ✓ La collecte de données « *sensibles* » est en principe interdite

⚠ Données sensibles : origine raciale ou ethnique, opinions politiques religieuses ou philosophiques, appartenance syndicale, santé, vie sexuelle

Exceptions : consentement de la personne, données rendues publiques, sauvegarde de la vie humaine, exercice d'un droit en justice, données nécessaires pour administrer des soins, …)

…appliqué au secteur social et médico-social (2/3)

- Données nécessaires au suivi et à l'accompagnement des personnes: elles sont **fonction des particularités des situations sociales rencontrées, du type de prestation ou de l'aide demandée et de la nature des actions individuelles et collectives à accomplir.**

  Exemple : diagnostic social ≠ aides « légales » (conditions d'attribution fixées par le(s) texte(s)

- Distinguer les informations à connaître de celles à enregistrer

Le responsable de traitement doit ainsi être en mesure de justifier du caractère nécessaire et proportionné des données à caractère personnel effectivement collectées dans le cadre de l'accompagnement réalisé.

FOCUS

- **NIR** : si justifié par un échange ou une facturation auprès de la sécurité sociale ou prévu par un texte
- **Données de santé** : en dehors du suivi médical, le traitement de données de santé pourra intervenir sous réserve du **consentement** de la personne concernée
- **Les zones de commentaires libres** : pour décrire une situation singulière - dans la mesure du possible, saisie des informations effectuée sous la forme de « cases à cocher » (champs libres à éviter) / informer les contributeurs du caractère objectif et strictement nécessaire des données à saisir (sensibilisation des employés)

3. Le principe d'une durée de conservation limitée

- ✓ Des données ne peuvent être conservées que le temps nécessaire à l'accomplissement de la finalité poursuivie (doctrine de la CNIL : pas plus de deux ans à compter du dernier contact)

- ✓ Archivage en cas de besoin

- ✓ Possibilité de conserver les données anonymisées

Chacun dispose d'un **droit à l'oubli**

5. L'obligation de sécurité (1/2)

« Le responsable du traitement est tenu de prendre toutes précautions utiles, ***au regard de la nature des données et des risques*** *présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »*

- ✓ Sécurité **organisationnelle** (analyse et gestion des risque, politique de sécurité des systèmes d'information, sensibilisation des utilisateurs), **physique** (alarme, site de secours, contrôle d'accès, vidéo, …) et **logique**
- ✓ Des obligations qui concerne aussi les **sous-traitants**

Habilitation interne

- Les personnes habilitées chargées de les traiter

- les destinataires et les tiers autorisés par un texte (il appartient au responsable de traitement de solliciter, auprès de l'organisme demandeur, le fondement légal autorisant ce dernier à obtenir des données)

- Les personnes concernées

Secret professionnel

4. Les droits des personnes

- ✓ Un droit à l'**information** (sur l'existence du traitement et ses caractéristiques) = une information claire des personnes sur des supports adaptés au regard du public concerné (affiches, dépliants, information délivrée par les travailleurs sociaux, publication sur le site internet, etc.)
- ✓ Un droit d'**accès** aux données (direct ou indirect)
- ✓ Un droit de **rectification** des données périmées
- ✓ Un droit d'**opposition pour motif légitime**

Dix questions à se poser avant de créer un fichier (1/2)

- ✓ Quel est le **but** de ce fichier ? (à quoi va-t-il servir?)
- ✓ Est-ce **légitime**, notamment au regard de mes missions et des droits des personnes?
- ✓ Comment présenter cette finalité pour la rendre compréhensible par tous ?
- ✓ Quelles sont les **données** dont j'ai forcément besoin pour atteindre l'objectif fixé ?
- ✓ Pendant **combien de temps** les données seront-elles utiles (évènement butoir, durée, obligations légales ou sauvegarde d'un droit en justice) ?

Dix questions à se poser avant de créer un fichier (2/2)

- ✓ Quels sont les membres de mon personnel qui ont besoin d'y **accéder** ?
- ✓ Existe-t-il des textes m'obligeant à les **archiver** ou à les communiquer à des organismes tiers ?
- ✓ Comment vais-je **informer** les personnes concernées par mon fichier et garantir leurs droits ?
- ✓ Au regard des risques et de la nature des données, quelles sont les mesures de **sécurité** à prévoir (mesures techniques et organisationnelles) ?
- ✓ Quelle est la **formalité** à accomplir auprès de la CNIL (déclaration ou autorisation) ?

Sécurité : quelques questions à se poser

- ✓ Le **contrôle d'accès** est-il adaptée ? (Habilitations, authentification, politique de mot de passe, traçabilité, …)
- ✓ La **sécurité physique** des locaux est-elle suffisante ? (Badges, sauvegardes, gardiennage)
- ✓ Les **échanges** avec des partenaires sont-ils sécurisés ?
- ✓ Quelle protection des données personnelles **échangées sur Internet** ? (Authentification, chiffrement des canaux, …)
- ✓ Quelle protection contre des **intrusions** externes par le réseau ? (Firewall, proxy, filtrage applicatif, détection d'intrusion, sécurité WIFI, …)
- ✓ Quelles garanties de **disponibilité** ? (Sauvegardes, redondance, plan de reprise, …)
- ✓ Quelle **confidentialité** des données par les **sous-traitants** ?
- ✓ Quelle protection pour les **données les plus sensibles** ? (Chiffrement, …)
- ✓ Les utilisateurs sont-ils **sensibilisés** aux risques informatiques ?

Le pack de conformité dédié à la sphère sociale et médico-sociale (1/3)

- ✓ Un **outil** pour comprendre et résoudre les difficultés rencontrées dans l'élaboration et la gestion des systèmes d'information
- ✓ Un outil **élaboré à la suite d'échanges** avec des acteurs du secteur
- ✓ Une **concertation** pour mieux appréhender les pratiques, les besoins et identifier les difficultés rencontrées
- ✓ Un outil qui se veut pérenne mais qui a vocation à évoluer avec le temps et les rapides évolutions du secteur

Le pack de conformité dédié à la sphère sociale et médico-sociale (2/3)

Trois outils de **simplification des formalités portant sur** :

- L'accueil et l'accompagnement des personnes handicapées et des personnes âgées
- L'accueil, l'orientation et l'accompagnement social
- La protection des mineurs et des jeunes majeurs

Le pack de conformité dédié à la sphère sociale et médico-sociale (3/3)

Un guide pédagogique pour aider les acteurs à mettre concrètement en application les principes « Informatique et Libertés » abordant notamment :

- ✓ L'**information** des personnes;
- ✓ Les **destinataires** des données et les **tiers autorisés**
- ✓ La **durée de conservation** des données et l'**archivage**
- ✓ L'utilisation des **zones de commentaires**
- ✓ Les **appréciations sur des difficultés sociales**
- ✓ Les données relatives aux **infractions** ou **condamnations**,
- ✓ Les données relatives à la **santé**
- ✓ Un volet sur l'accompagnement dans la conformité « étape par étape ».

Merci de votre attention

****

Des questions?