



FNARS
agir pour la solidarité

**LA DEMARCHE DE MISE EN CONFORMITE
ET SES IMPACTS**

16 Mars 2017
Journée professionnelle de l'UNAFO

Intervenante: Carole Lardoux

A quelles difficultés notre secteur est-il confronté?

Les difficultés du secteur

- ▶ Utilisation de fichiers non sécurisés : Excel, Access...
- ▶ Envois non sécurisés d'informations : mails, sms, fax
- ▶ Pression de partenaires externes pour obtenir des listings nominatifs de personnes
- ▶ Manque de confiance vis-à-vis des professionnels
- ▶ Manque d'informations à destination des personnes prises en charge
- ▶ Manque d'informations à destination des professionnels et bénévoles
- ▶ Difficulté de mise en œuvre des préconisations de la CNIL
- ▶ Envie de tout connaître, tout analyser ... sans prendre en compte le droit des personnes

L'Autorisation Unique « AU 48 »

3 autorisations uniques

- ▶ **Adoption de plusieurs autorisations uniques : 14/04/16**
- ▶ **Objectifs:**
 - ▶ simplifier les démarches pour les acteurs de terrain
 - ▶ Faire respecter la conformité dans le secteur social et médico-social
- ▶ **AU 48 : Accompagnement et suivi social des personnes en difficultés**
- ▶ **AU 47 : Accompagnement et suivi social et médico-social des personnes handicapées et des personnes âgées**
- ▶ **AU 49 : Accompagnement et suivi social dans le cadre de la prévention et de la protection des mineurs et jeunes majeurs**

Les 5 règles d'or de la protection des données

▶ Une finalité du traitement déterminée, explicite et légitime :

Correspondant aux missions de l'organisme

Un fichier ne doit pas servir à d'autres fins que celles pour lesquelles il a été prévu (détournement de finalité= 5 ans d'emprisonnement, 300 000 euros d'amende)

▶ Des données adéquates, pertinentes, non excessives et mises à jour.

Elles doivent être nécessaires et proportionnées au regard de la finalité poursuivie.

▶ Une durée de conservation des données limitée: droit à l'oubli

Les 5 règles d'or de la protection des données

► Le respect des droits des usagers:

Information des personnes, lors du recueil, de l'enregistrement ou au plus tard de la première communication des données de :

-la finalité du traitement, du caractère obligatoire ou facultatif des réponses et des conséquences d'un défaut de réponse; de l'identité du responsable du traitement; des destinataires des données,

-Et de leurs droits : d'accès et de rectification, d'opposition (sauf obligation légale) aux informations collectées

► Des mesures de sécurité adaptées : confidentialité, intégrité et pérennité des données

Prise de précautions pour préserver **l'intégrité et la confidentialité** des données: mots de passe régulièrement changés, éteindre les ordinateurs, politique de gestion des habilitations d'accès aux données et traçabilité des accès

L'AU 48

▶ Qui est concerné?

Les organismes, services et établissements (CHRS, CHU, accueil de jour, SIAO, SAO, services d'accompagnement, ACT, LHSS etc...) doivent répondre à cet **engagement de conformité**

▶ Comment déclarer?

Déclaration en ligne sur le site de la CNIL

▶ Quelles sont les informations déclarées?

Les finalités prévues pour la collecte des données, les données personnelles pouvant être traitées, les droits des personnes, et les mesures de sécurité nécessaires à la protection de données à caractère personnel.

L'AU 48

► Que faire en cas de collecte d'informations non prévues dans l'AU 48?

L'organisme doit faire une demande d'autorisation à la CNIL.

Exemple : lorsque les traitements comportent le numéro de sécurité sociale des personnes.

► Outil complémentaire

Ces autorisations uniques seront prochainement suivies d'un guide sous forme de fiches pratiques pour expliquer de façon pédagogique les règles relatives à la protection des données personnelles (Pack social).

Pack social pour le logement

2 AVANT PROPOS

3 LE CADRE GÉNÉRAL DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

4 DÉFINITIONS DES NOTIONS CLÉS

5 LES PRINCIPES À RESPECTER

Le principe d'une finalité légitime (article 6-2°)

Les principes de pertinence et de proportionnalité des données collectées (article 6-3°)

Le principe d'une durée limitée de conservation des données (article 6-5°)

Le principe de sécurité et de confidentialité des données (article 34)

6 L'INFORMATION ET LES DROITS DES PERSONNES

L'information des personnes (article 32)

Les droits des personnes

9 LES FORMALITÉS PRÉALABLES À LA MISE EN PLACE D'UN FICHER

La déclaration normale

La dispense de déclaration

Les procédures simplifiées

Le régime de l'autorisation

Pack social pour le logement

12 LE CORRESPONDANT INFORMATIQUE ET LIBERTÉS : UN VECTEUR DE MISE EN CONFORMITÉ ET DE DIFFUSION DE LA CULTURE INFORMATIQUE ET LIBERTÉS

13 FICHES PRATIQUES

- 13 **FICHE N°1** : LES OUTILS DE SIMPLIFICATION DES FORMALITÉS DU PACK DE CONFORMITÉ DÉDIÉ AU LOGEMENT SOCIAL
- 16 **FICHE N°2** : PERSONNES HABILITÉES, SOUS-TRAITANTS, DESTINATAIRES DES DONNÉES ET TIERS AUTORISÉS
- 22 **FICHE N°3** : DURÉE DE CONSERVATION ET ARCHIVAGE DES DONNÉES
- 25 **FICHE N°4** : LA VIDÉOSURVEILLANCE ET LA VIDÉOPROTECTION DANS LES ENSEMBLES IMMOBILIERS À CARACTÈRE SOCIAL
- 30 **FICHE N°5** : L'UTILISATION DES CHAMPS LIBRES ET ZONES DE COMMENTAIRES
- 34 **FICHE N°6** : LE TRAITEMENT D'APPRÉCIATIONS SUR LES DIFFICULTÉS SOCIALES
- 38 **FICHE N°7** : LE TRAITEMENT DE DONNÉES RELATIVES À LA SANTÉ
- 41 **FICHE N°8** : LES DONNÉES RELATIVES À DES INFRACTIONS, CONDAMNATIONS OU MESURES DE SÛRETÉ
- 45 **FICHE N°9** : L'INFORMATION DES PERSONNES
- 47 **FICHE N°10** : SÉCURITÉ DES DONNÉES

Pack social pour le logement

● UNE NORME SIMPLIFIÉE MISE À JOUR

Parmi les organismes et personnes susceptibles de recevoir des données de la part d'un bailleur social, on doit donc distinguer :

- les membres de son personnel chargés de traiter les données en raison de leurs fonctions, qualifiés comme étant des « personnes habilitées à y accéder »,
 - les sous-traitants,
 - les destinataires des données, soit les personnes ou organismes extérieurs auxquels le responsable de traitement transmet des données de sa propre initiative, à l'exclusion des sous-traitants, ou à la suite d'une demande non prévue par la loi qu'il estime légitime,

- les « tiers autorisés », c'est-à-dire les personnes ou organismes pouvant obtenir la communication de données en vertu d'une disposition législative ou réglementaire.

L'accès aux données par les employés habilités d'un bailleur

Les employés habilités d'un responsable de traitement ne sont pas des destinataires au sens de la loi « Informatique et Libertés ».

L'accès aux données contenues dans les fichiers d'un bailleur par son personnel obéit



Illustration : finalités du traitement

- ▶ **Accompagnement et suivi des personnes : accès aux droits, éducatif et budgétaire, demandes d'aide sociale...**
- ▶ **Saisie de problématiques identifiées dans le cadre de l'évaluation sociale**
- ▶ **Gestion des demandes d'hébergement et d'accès au logement**
- ▶ **Gestion des impayés et prévention des expulsions locatives**
- ▶ **Échange et partage d'informations entre intervenants sociaux, médicaux et paramédicaux afin de garantir la coordination et la continuité de l'accompagnement et du suivi des personnes**
- ▶ **Etablissement de statistiques, études internes et d'enquêtes de satisfaction aux fins d'évaluation des activités, de la qualité des prestations et des besoins à couvrir**

Illustration : données à caractère personnel

- ▶ **Données d'identification des bénéficiaires**
- ▶ **Problématiques identifiées dans le cadre de l'évaluation sociale**
- ▶ **Informations relatives à la procédure de demande d'asile (dépôt d'une demande d'asile : oui/non) ainsi que les informations nécessaires à l'élaboration du récit de vie**
- ▶ **Informations relatives à la vie personnelle du bénéficiaire**
- ▶ **Conditions de vie matérielles**
- ▶ **Données d'identification des personnes concourant à l'accompagnement et suivi social : nom, prénom, qualité, organisme d'appartenance, numéro de téléphone, adresse professionnelle, courriel, téléphone**

Illustration : destinataires possibles

- ▶ **Personnel concourant à la prise en charge, à l'accompagnement et au suivi social et médico-social** des personnes
- ▶ **Professionnels et tout membre du personnel** de l'établissement, du service ou organisme externe, **particiant à la prise en charge, à l'accompagnement et au suivi** de la personne, **et toute autre personne en relation, de par ses activités**, avec ces établissements ou organismes externes, **dans la limite de leurs attributions respectives et des règles encadrant le partage et l'échange d'informations**
- ▶ **Organismes instructeurs et payeurs de prestations sociales**
- ▶ **Organismes financeurs et gestionnaires** s'agissant exclusivement de données préalablement anonymisées à l'exception de ceux autorisés par une disposition légale ou réglementaire à obtenir la communication de données à caractère personnel relatives aux personnes visées par la présente autorisation unique.

=> Respect de **l'attribution légale** et **chacun a accès** uniquement aux informations qui le concernent

Toute demande d'informations en vue d'une étude statistique fera l'objet d'une transmission de données préalablement anonymisées.

La durée de conservation des données

- ▶ **Conservation dans la base active des données collectées et traitées de deux ans à compter du dernier contact avec la personne**
- ▶ **Les justificatifs recueillis, y compris sous format papier, qui n'ont plus d'utilité, soit parce qu'ils sont trop anciens pour justifier de la situation de l'utilisateur, soit parce que le dossier pour lequel ils ont été demandés est constitué, doivent être détruits**
- ▶ **les données doivent être supprimées sans délai en cas de décès de la personne concernée**

L'obligation d'information des personnes

- ▶ **Information des personnes par tout moyen approprié**, dans un langage compréhensible et selon des modalités appropriées et adaptées à leur état
- ▶ Informations sur **l'identité du responsable de traitement**, la **finalité** poursuivie par le traitement, **les destinataires des données et les droits des personnes** (droits d'opposition pour motifs légitimes, d'accès et de rectification)
- ▶ **Information du caractère obligatoire ou facultatif des réponses** + conséquences éventuelles, d'un défaut de réponse ou de l'exercice de leur droit d'opposition
- ▶ Information mentionnée **sur les formulaires de collecte**
- ▶ Les **droits d'opposition**, pour motifs légitimes, **d'accès et de rectification s'exercent directement** auprès du ou des services que le responsable de traitement doit impérativement désigner

Les mesures de sécurité

- ▶ **Par internet: mesures adéquates permettant de garantir la confidentialité des données échangées, telles qu'un chiffrement des données**
- ▶ **Authentification au moyen d'un identifiant et d'un mot de passe personnels**
- ▶ **Gestion des habilitations**
- ▶ **Traçabilité des accès**
- ▶ **Externalisation de l'hébergement de données de santé à caractère personnel**
- ▶ **Mécanismes de traitement automatique garantissant que les données à caractère personnel seront systématiquement supprimées, à l'issue de leur durée de conservation, ou feront l'objet d'une procédure d'anonymisation rendant impossible toute identification ultérieure des personnes concernées**
- ▶ **Mécanisme d'anonymisation pour le traitement statistique**