# PACK DE CONFORMITÉ

# LOGEMENT SOCIAL

CNIL
Commission Nationale de l'Informatique et des Libertés

Édition juillet 2014

cnil.fr

# SOMMAIRE

PACK DE CONFORMITÉ

# LOGEMENT SOCIAL

## AVANT PROPOS

***Les récentes et rapides évolutions de l'environnement numérique ont amené la CNIL à repenser son action et ses outils d'intervention. Elle souhaite désormais associer et responsabiliser les acteurs des différents secteurs qu'elle doit réguler.***

*Cela ne peut se faire qu'en proposant des outils permettant de mettre en œuvre concrètement, et le plus en amont possible, les principes «Informatique et Libertés».*

*Qu'il s'agisse de codes de bonne conduite ou bonnes pratiques, de chartes, de labels, de pack de conformité, de réseaux de correspondants informatique et libertés, ces leviers ont vocation à être au service de la conformité des organismes, en étant ancrés dans la réalité et les spécificités du secteur, efficaces et pérennes dans le temps.*

*Les incompréhensions suscitées par une mise en demeure publique prononcée à l'encontre d'un bailleur social ont amené la CNIL à engager une réflexion pour comprendre et résoudre les difficultés rencontrées dans l'élaboration et la gestion des systèmes d'information des bailleurs sociaux.*

*Une concertation avec certains des acteurs de ce secteur a permis à la CNIL de mieux appréhender leurs pratiques, leurs besoins et d'identifier les difficultés qu'ils rencontrent pour mettre en œuvre des traitements de données à caractère personnel conformes à la loi « Informatique et Libertés ».*

*Ce chantier a abouti à l'adoption d'un pack de conformité dédié au secteur, dont ce guide est l'un des éléments constitutifs.*

**Ce pack de conformité comprend :**

- *Trois outils de simplification des formalités à accomplir par les bailleurs auprès de la CNIL, à savoir :*
  - *une mise à jour en profondeur de la norme simplifiée n° 20 pour déclarer plus facilement les traitements de données à caractère personnel visant à enregistrer et instruire les demandes de logement social, d'une part, et à assurer une gestion courante du patrimoine immobilier, d'autre part ;*
  - *une nouvelle autorisation unique autorisant les bailleurs sociaux à mettre en œuvre des traitements comportant des appréciations sur des difficultés sociales des résidents aux fins d'attribution, d'adaptation et de mutation des logements ou, si les personnes concernées le souhaitent, de mise en place d'un suivi social personnalisé ;*
  - *une nouvelle autorisation unique concernant la gestion du précontentieux et du contentieux et permettant également de traiter des décisions de justice lorsqu'elles ont une incidence sur un lieu de résidence ;*

- *Le guide pédagogique qui a vocation à évoluer dans le temps, élaboré pour aider les bailleurs à mettre concrètement en application les principes « Informatique et Libertés ». Ce guide aborde les thèmes suivants :*
  - *l'information des résidents ;*
  - *les destinataires des données et les tiers autorisés ;*
  - *la durée de conservation des données et l'archivage ;*
  - *la bonne utilisation des zones de commentaires ;*
  - *le traitement d'appréciations sur des difficultés sociales, d'infractions ou de condamnations, ou encore de données relatives à la santé.*

Pour accomplir leurs missions, les bailleurs sociaux utilisent dans la plupart des cas des fichiers informatiques, que ce soit pour instruire les demandes de logement, gérer leur patrimoine immobilier ou assurer d'autres tâches plus spécifiques, telles que proposer un suivi social à certains résidents.

Dès lors que ces fichiers contiennent des données permettant d'identifier directement ou indirectement au moins une personne physique (par référence à son nom, son adresse, son numéro de téléphone, sa photographie, un numéro unique, …), ils sont soumis aux dispositions de la loi du 6 janvier 1978 modifiée, dite loi « Informatique et Libertés ».

Pour prévenir toute atteinte aux libertés individuelles et à la vie privée des personnes, la loi « Informatique et Libertés » définit les principes et les règles à respecter lors de la collecte, du traitement, de la conservation et de la transmission des données à caractère personnel.

Elle prévoit également un certain nombre de droits pour les personnes dont les données ont été recueillies.

La Commission nationale de l'informatique et des libertés (CNIL), autorité administrative indépendante, est chargée d'assurer le respect de cette loi.

**PRÉCISION**

La loi « Informatique et Libertés » s'applique aux fichiers informatisés, mais également aux traitements non automatisés de données à caractère personnel, quand les données sont contenues ou appelées à figurer dans un ensemble structuré et stable accessibles selon des critères déterminés (exemple : des dossiers papiers classés par ordre alphabétique ou chronologique).

Elle informe les personnes quant à l'existence et aux modalités pratiques d'exercice de leurs droits et rappelle leurs obligations aux organismes qui mettent en œuvre des fichiers.

La CNIL vérifie ainsi, lors de l'accomplissement de formalités par les organismes, que les caractéristiques de leurs fichiers sont conformes aux dispositions de la loi « Informatique et Libertés ».

Pour s'assurer du respect de la loi, la CNIL dispose d'un pouvoir de contrôle sur place et sur pièces, ainsi que d'un pouvoir de sanction.

# 01 LE CADRE GÉNÉRAL DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

## DÉFINITIONS DES NOTIONS CLÉS

La loi « Informatique et Libertés » définit une **donnée à caractère personnel** comme toute information relative à une personne physique identifiée ou identifiable, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Un **traitement de données à caractère personnel** est quant à lui défini comme toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, …).

La loi précise qu'un **fichier** de données à caractère personnel est un ensemble structuré et stable de données accessibles selon des critères déterminés.

Le **responsable d'un traitement** de données à caractère personnel est, sauf désignation expresse par une disposition législative ou réglementaire, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités (c'est-à-dire ses objectifs) et ses moyens.

La **personne concernée** par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement.

Enfin, **le destinataire** d'un traitement de données à caractère personnel est toute personne habilitée à recevoir communication de ces données autres que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données.

**PRÉCISION**

Les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander à un responsable de traitement la communication de données à caractère personnel ne sont pas des destinataires.

Ces autorités sont usuellement désignées comme des **tiers autorisés** (Cf. Fiche n° 2).

## LES PRINCIPES CLÉS À RESPECTER

La loi « Informatique et Libertés » définit les principes qu'un responsable de traitement doit respecter lors de la collecte, du traitement ou encore de la conservation des données.

Elle garantit par ailleurs un certain nombre de droits pour les personnes concernées.

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

Des données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé, explicite et légitime.

La finalité d'un traitement doit logiquement correspondre aux missions de l'organisme qui envisage de le mettre en place.

Les objectifs poursuivis par le responsable du traitement doivent donc être préalablement définis, de manière claire, explicite et exhaustive.

Par exemple : un fichier qui concerne les dossiers des résidents d'un ensemble immobilier ne doit servir qu'à la gestion du parc. Les informations ne peuvent en principe être utilisées à des fins de prospection commerciale ou politique.

Toute utilisation d'une donnée à caractère personnel pour un objectif incompatible avec la finalité première du traitement est un détournement de finalité passible de sanctions administratives ou pénales.

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

Seules doivent être traitées les informations pertinentes, adéquates et non excessives au regard de la finalité du fichier, c'est-à-dire de son objectif.

Par exemple : l'enregistrement de données relatives à des difficultés sociales n'est pas pertinent, sauf si les informations demandées sont indispensables pour une prise en charge dans le cadre d'un suivi social proposé par un bailleur.

De la même manière, la nature d'un handicap ne doit être renseignée que si cette information a une incidence sur les caractéristiques du logement, d'une part, et qu'il n'est pas possible de se limiter à la collecte d'une donnée plus générale, d'autre part (principe de minimisation des données).

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

Des données à caractère personnel ne peuvent être conservées de façon indéfinie dans un fichier.

Une durée de conservation précise doit impérativement être déterminée, en fonction de la finalité de chaque fichier, par le responsable du traitement.

**PRÉCISION**

Une durée de conservation peut renvoyerà une durée fixe exprimée en jours, en moisou en année. Mais elle peut également s'exprimer par référence à un évènement butoir (durée d'une relation contractuelle, durée de la prescription applicable, …).

Par exemple, des données collectées pour instruire une demande de logement social doivent être supprimées en cas de radiation de la demande correspondante, dans la mesure où ces données ne présentent plus d'intérêt par rapport à cette finalité.

En cas d'attribution d'un logement, les données collectées pour instruire la demande peuvent être conservées et utilisées dans un fichier servant à gérer le patrimoine, sous réserve de présenter un caractère indispensable et d'en avoir informé le résident concerné. Dans cette hypothèse, les données peuvent être conservées jusqu'au départ du résident concerné ou, en cas de sommes restant à payer, à compter du paiement complet des sommes dues au bailleur.

Des dispositions législatives ou réglementaires peuvent toutefois contraindre un responsable de traitement à conserver des données au-delà de leur durée de conservation en base active.

Dans ce cas, les données peuvent être conservées dans une base d'archive, le temps nécessaire au respect de l'obligation en question, dans le respect des conditions prévues par la délibération de la CNIL relative aux modalités d'archivage électronique dans le secteur privé (délibération n°2005-213 du 11 octobre 2005), ou des dispositions du code du patrimoine prescrivant aux gestionnaires de logement sociaux de verser des documents à un service d'archivage départemental.

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

Le responsable du traitement est astreint à une obligation de sécurité : il doit notamment prendre les mesures nécessaires pour garantir la confidentialité des données qu'il a collectées et éviter leur divulgation à des tiers non autorisés.

L'accès aux données ne doit ainsi être ouvert qu'aux employés habilités à en connaître en raison de leurs fonctions.

Chaque personne doit disposer d'un identifiant et d'un mot de passe individuel. Les droits permettant d'accéder aux données doivent être précisément définis en fonction des besoins réels de chaque utilisateur.

Il est également recommandé de prévoir un mécanisme de verrouillage systématique des postes informatiques, au-delà d'une courte période d'inactivité, ainsi qu'un dispositif de traçabilité des connexions aux applications permettant de s'assurer qu'aucun agent n'a accédé à des données en dehors de ses missions, notamment par simple curiosité.

Avant de communiquer des données à un organisme extérieur, un bailleur social doit ainsi se poser un certain nombre de questions (Cf. fiche n° 2 destinataire des données et tiers autorisés), en particulier quant au respect des droits des résidents (*Voir fiche n°9*).

Les données peuvent également être communiquées à des tiers autorisés à en connaître en application de dispositions législatives ou règlementaires particulières (commission de médiation dite DALO, commission d'attribution, autorités judiciaires, services fiscaux, services de police ou de gendarmerie, …).

Dans ce cas, le responsable du fichier doit toutefois s'assurer du caractère obligatoire du texte utilisé à l'appui de la demande de l'organisme tiers autorisé, et ne transmettre que les données prévues par le texte ou, si ce dernier ne les liste pas, les seules données indispensables au regard de la finalité du droit de communication en question.

## L'INFORMATION ET LES DROITS DES PERSONNES

Toute personne dont les données sont contenues dans un fichier doit en être préalablement informée.

Elle dispose également du droit de s'y opposer pour un motif légitime, d'accéder à ses données, ainsi que de les faire rectifier ou supprimer.

Ces droits doivent impérativement être pris en compte par les bailleurs sociaux.

### L'information des personnes (article 32)

Lors de la collecte de données à caractère personnel, qu'il s'agisse d'un traitement automatisé ou non, les personnes concernées (résidents, employés, entreprises intervenantes, ...) doivent être clairement informées :

- de l'identité du responsable de traitement ou de son représentant,
- des objectifs poursuivis par le traitement,
- du caractère obligatoire ou facultatif des réponses,
- des conséquences éventuelles d'un défaut de réponse,
- des destinataires ou catégories de destinataires des données,
- de l'existence de droits à leur profit (droit d'opposition pour motif légitime, droit d'accès aux données les concernant, droit de rectification et de suppression) et des coordonnées du service ou de la personne qui doit répondre aux demandes,
- le cas échéant, des transferts de données effectuées vers des pays non membres de l'Union européenne (pays d'établissement des destinataires, nature des données transférées, finalité du transfert, catégories de destinataires, niveau de protection offert par le(s) pays tiers).

Cette information peut être diffusée par tout moyen que le responsable de traitement estime approprié.

Lorsque des données sont recueillies par voie de questionnaire, ces derniers doivent impérativement porter mention de l'identité du responsable de traitement ou de son représentant, de la finalité du traitement, du caractère obligatoire ou facultatif des réponses et des droits qui leur sont reconnus (article 32-I).

**PRÉCISION**

Le site internet de la CNIL donne accès à un outil permettant de générer différents types de modèles de mentions légales.

Ces modèles, modifiables pour permettre à un bailleur social de les adapter à ses besoins sont accessibles à l'adresse suivante : http://www.cnil.fr/vos-obligations/informations-legales/

Lorsque des données sont recueillies lors d'un entretien, il convient de remettre ou de faire préalablement parvenir aux personnes concernées un document contenant l'information en caractères lisibles.

En cas d'information par voie d'affichage ou par téléphone, l'information délivrée doit également préciser aux intéressés qu'ils peuvent, sur simple demande, recevoir postérieurement ces informations sur un support écrit.

**PRÉCISION**

Avec l'accord des personnes concernées, les informations écrites peuvent être communiquées par voie électronique.

### Les droits des personnes

La loi « Informatique et Libertés » reconnait des droits aux personnes dont les données figurent dans un fichier.

#### 1. Le droit d'accès (article 39 de la loi)

Toute personne physique justifiant de son identité peut interroger le responsable d'un traitement de données en vue d'obtenir :

- la confirmation que des données le concernant font ou ne font pas l'objet d'un traitement ;

- des informations sur la finalité d'un traitement et les catégories de données traitées, ainsi que sur les destinataires ou catégories de destinataires auxquelles les données sont communiquées ;
- le cas échéant, des informations sur les transferts de données hors de l'Union européenne ;
- la communication, sous une forme accessible, des données le concernant ainsi que toute information disponible quant à leur origine ;
- des informations permettant de connaitre et de contester la logique du traitement en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à son égard.

Un résident peut ainsi demander et obtenir sur simple demande, sauf disposition législative ou réglementaire contraire, la communication d'une copie de toutes les données le concernant et figurant dans les différents fichiers de son bailleur (dossier individuel, zones de commentaires, enregistrements vidéos…). Un bailleur peut demander à cette occasion la production d'un justificatif d'identité.

**PRÉCISION**

Les codes, sigles et abréviations figurant dans les documents délivrés par un bailleur en réponse à une demande de droit d'accès doivent être expliqués au demandeur, si nécessaire sous la forme d'un lexique.

**PRÉCISION**

La communication de données implique nécessairement la protection des données des tiers, y compris en cas de consultation sur place.

Ainsi, il convient par exemple de flouter ou couper des parties d'enregistrements vidéos pour rendre les tiers non identifiables.

La demande d'accès peut s'effectuer, au choix du demandeur, par écrit ou sur place. Lorsque le bailleur n'est pas en mesure de satisfaire immédiatement à la demande, celui-ci délivre au demandeur un avis de réception daté et signé. Il dispose d'un délai de deux mois pour répondre à la demande d'accès.

Le bailleur peut subordonner la délivrance d'une copie au paiement d'une somme qui ne peut excéder le coût de la reproduction. En cas de facturation, il doit attester du paiement de la somme perçue.

La loi prévoit que le responsable de traitement ne peut s'opposer qu'aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique (article 39-II).

En cas de contestation, il appartient au responsable de traitement de démontrer le caractère abusif de la demande.

**FOCUS**

***La mise à jour de données à l'initiative d'un bailleur***

Un bailleur est légitimement fondé à mettre en place une politique de mise à jour des données concernant ses résidents.

Cette politique peut être autonome (envoi d'un courrier spécifique accompagné d'un coupon réponse, déplacement au domicile des personnes, appel téléphonique…) ou être réalisée à l'occasion d'un autre évènement, notamment pour rationnaliser les coûts (enquête sur l'occupation du parc social, autre enquête obligatoire…).

Dans ce dernier cas, les résidents doivent être clairement informés des deux finalités distinctes poursuivies par le bailleur (*par exemple : réalisation d'une enquête obligatoire + mise à jour des données de leurs dossiers*), ainsi que du caractère obligatoire ou facultatif des réponses et des conséquences qui peuvent en résulter.

### 2. Le droit de rectification

Toute personne justifiant de son identité a le droit d'exiger que les données la concernant soient rectifiées, complétées, mises à jour, verrouillées ou effacées (article 40 de la loi).

Lorsqu'un bailleur est confronté à une demande de rectification ou de suppression de données, il doit pouvoir justifier, sans frais pour le résident, qu'il a procédé aux opérations demandées.

Par ailleurs, lorsque les données ont été transmises à un tiers, le bailleur ayant procédé à leur rectification doit également en informer ce destinataire sans délai, lequel doit à son tour modifier son traitement.

Si un résident a payé une somme pour la reproduction de données dans le cadre de son droit d'accès, il peut obtenir le remboursement de ces frais lorsque les données doivent être mises à jour.

Les héritiers d'un résident décédé justifiant de leur identité peuvent, s'ils supposent que des données en rapport avec le défunt ne sont plus à jour, exiger d'un bailleur qu'il prenne en compte ce décès et mette à jour son traitement.

De la même façon, le bailleur doit pouvoir justifier, sans frais pour les héritiers, qu'il a procédé aux opérations demandées.

**PRÉCISION**

Au delà de la justification de son identité, l'héritier d'un résident décédé souhaitant mettre à jour les données relatives au défunt doit, à l'occasion de la demande, apporter la preuve de sa qualité d'héritier par la production d'un acte de notoriété ou d'un livret de famille.

### 3. Le droit d'opposition pour motif légitime

Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données la concernant soient enregistrées dans un fichier informatique, sauf si celui-ci résulte d'une obligation légale (article 38 de la loi).

En particulier, tout résident est en droit de s'opposer, sans frais, à ce que des données le concernant soient utilisées à des fins de prospection, notamment commerciale, par son bailleur ou le responsable d'un traitement ultérieur.

Enfin, le responsable d'un traitement auprès duquel un droit d'opposition a été exercé doit informer, sans délai, les destinataires de son traitement quant à cette opposition, en particulier sur les données faisant l'objet de l'opposition.

**PRÉCISION**

En cas de collecte de données à distance, notamment par l'intermédiaire d'un intranet ou d'internet, les résidents doivent être en mesure d'exprimer leur opposition au traitement de leurs données à des fins de prospection avant la validation définitive de leurs réponses.

Par ailleurs, en cas de collecte par oral, l'intéressé doit être en mesure d'exercer son droit d'opposition avant la fin de la collecte.

### 4. Règles communes aux droits des personnes

Lorsqu'une demande de droit d'accès, de rectification, de suppression ou d'opposition est présentée par écrit par un résident, la demande doit être signée et accompagnée de la photocopie d'un titre d'identité portant la signature du titulaire.

Cette demande doit préciser l'adresse à laquelle le bailleur doit faire parvenir sa réponse.

En cas de doute sur l'adresse ou l'identité du demandeur, la réponse du bailleur peut être expédiée sous pli recommandé sans avis de réception, la vérification de l'adresse ou de l'identité s'effectuant lors de la délivrance du pli.

Lorsque le responsable de traitement n'est pas connu d'un résident, ce dernier peut adresser sa demande au siège de la personne morale.

En cas de demande présentée sur place, un résident doit justifier par tout moyen de son identité. Il peut également se faire assister d'un conseil de son choix.

Une demande peut également être présentée par une personne spécialement mandatée à cet effet par un résident. Dans ce cas, le mandataire doit justifier de son mandat, de son identité et de celle de son mandant.

Lorsqu'une demande ne peut être satisfaite immédiatement par un bailleur, ce dernier doit délivrer au résident un avis de réception daté et signé.

Un bailleur dispose d'un délai de deux mois pour répondre aux demandes de ses résidents, à compter de la date de réception de la demande.

Si la demande est imprécise ou ne comporte pas tous les éléments permettant au bailleur de procéder aux opérations demandées, il doit inviter le demandeur à lui fournir ces éléments avant l'expiration du délai de deux mois précité. Le bailleur procède à cette démarche par lettre remise contre signature ou par voie électronique, étant précisé que la demande de compléments suspend le délai dont dispose le bailleur pour répondre.

Sauf pour les demandes manifestement abusives, la décision de ne pas donner suite à une demande doit être motivée par le bailleur. Les voies et délais de recours ouverts pour contester cette décision doivent également être mentionnés.

**PRÉCISION**

Le silence gardé pendant deux mois par un bailleur vaut décision de refus.

## LES FORMALITÉS PRÉALABLES À LA MISE EN PLACE D'UN FICHIER

Tout fichier contenant des données à caractère personnel, c'est-à-dire celles permettant d'identifier directement ou indirectement au moins une personne physique, doit faire l'objet d'une formalité auprès de la CNIL préalablement à sa mise en œuvre, sauf s'il en est spécifiquement exonéré.

Les formalités à accomplir (déclaration, demande d'autorisation ou demande d'avis) dépendent de la finalité du traitement et de la nature des données collectées.

**PRÉCISION**

Déclarer un fichier de données personnelles est une obligation légale dont le non respect est susceptible d'être sanctionné administrativement ou pénalement.

Toutes les formalités peuvent être effectuéesen ligne sur le site internet de la CNIL. En cas de doute sur le régime dont relèvent le traitement ou sur vos obligations, vous pouvez interroger les services de la CNIL.

Certains traitements sont dispensés de formalités ou peuvent faire l'objet de procédures allégées.

Avant de procéder aux formalités, il convient donc de vérifier si le fichier concerné est exonéré de déclaration, ou s'il peut faire l'objet d'un engagement de conformité à une norme simplifiée, à une autorisation unique ou à un acte règlementaire unique.

### La déclaration normale

Pour les fichiers qui ne relèvent pas d'une procédure spécifique (Cf. infra), le régime de formalité de droit commun est la déclaration normale.

Une seule déclaration ne peut viser des finalités différentes. Dans ce cas, il convient de faire autant de déclarations que de finalités.

Le fichier peut être mis en place dès réception du récépissé de déclaration adressé par la CNIL, qui atteste que le dossier est considéré comme complet.

Ce récépissé certifie de l'accomplissement de la formalité, mais il n'exonère pas le responsable de traitement de ses obligations

de fond (respect de la finalité du fichier, ne pas collecter de données excessives, respecter les droits des personnes, prévoir les mesures de sécurité nécessaires…).

**PRÉCISION**

La désignation d'un Correspondant Informatique et Libertés (CIL) permet un allègement des formalités de déclaration.

Elle est également un moyen efficace de veiller à une bonne connaissance et à une bonne application de la loi.

Les déclarations peuvent être effectuées directement sur le site internet de la CNIL, à l'adresse suivante : http://www.cnil.fr/vos-obligations/declarer-a-la-cnil/

### La dispense de déclaration

La CNIL peut dispenser de déclaration les fichiers qui ne sont pas susceptibles de porter atteinte à la vie privée des personnes.

Pour bénéficier de cette exonération, le fichier doit être conforme au texte de la dispense (http://www.cnil.fr/en-savoir-plus/deliberations/dispenses-de-declaration).

**PRÉCISION**

La dispense de déclaration n'exonère par le responsable de traitement des obligations de la loi « Informatique et Libertés », telles que l'information des personnes ou la sécurité des données.

Le traitement automatisé de la comptabilité générale fait ainsi l'objet d'une dispense de déclaration (délibération de la CNIL n° 80-34 du 21 octobre 1980).

De la même manière, les traitements de gestion des rémunérations du personnel sont dispensés de déclaration (dispense n° 1 pour le secteur public ; dispense n° 2 pour le secteur privé).

Les traitements mis en œuvre dans le cadre de la dématérialisation de marchés publics bénéficient également d'une dispense (dispense n° 3), de même que les traitements relatifs à la gestion des fichiers de fournisseurs comportant des personnes physiques (dispense n° 4).

Cette liste n'est toutefois pas exhaustive et d'autres dispenses peuvent intéresser les bailleurs sociaux (plan de continuité en cas de pandémie grippale, information et communication externe s'il ne s'agit pas de sollicitions commerciales, …).

### Les procédures simplifiées

Pour certains des fichiers les plus courants, la CNIL a adopté des cadres de référence qui définissent les finalités, les données qui peuvent être collectées et les modalités de mise en œuvre du traitement afin de simplifier les formalités à accomplir.

Le responsable de traitement doit s'assurer que les caractéristiques de son traitement correspondent en tous points au cadre de référence qui est d'interprétation stricte (norme simplifiée, autorisation unique ou acte réglementaire unique : http://www.cnil.fr/en-savoir-plus/deliberations).

Si tel est le cas, il peut effectuer un engagement de conformité à ce texte (déclaration simplifiée).

Un bailleur social peut ainsi se référer à la norme simplifiée n° 46 pour déclarer un traitement mis en œuvre pour la gestion de son personnel.

S'agissant d'un traitement visant à gérer des demandes de logement social ou un patrimoine immobilier à caractère social, la norme simplifiée n° 20 (gestion des demandes et du parc immobilier) permet aux bailleurs sociaux de déclarer plus facilement ce type de fichiers.

### Le régime de l'autorisation

Les traitements de données à caractère personnel qui présentent des risques particuliers doivent être autorisés par la CNIL.

Pour connaitre la liste intégrale des types de fichiers qui doivent faire l'objet d'une auto-

risation de la CNIL, il convient de lire l'article 25 de la loi « Informatique et Libertés ».

Il s'agit notamment des traitements comportant des données dites « sensibles », c'est à dire celles faisant apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou bien fournissant des informations relatives à la santé (sauf en cas de recueil d'un consentement exprès) ou à la vie sexuelle de celles-ci.

Le régime de l'autorisation concerne aussi les fichiers qui comportent des appréciations sur des difficultés sociales, qui portent sur le numéro de sécurité sociale (sauf pour la gestion de la paie, pour les déclarations sociales obligatoires ainsi que dans le cadre de la prise en charge des frais de santé) ou ceux qui portent sur des infractions, des condamnations ou des mesures de sûreté.

Tel est également le cas des fichiers d'exclusion qui, du fait de leur nature, de leur portée ou de leurs finalités, sont susceptibles d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire.

Les fichiers mis en œuvre par un bailleur dans le cadre d'un accompagnement social sont susceptibles de contenir des appréciations sur les difficultés sociales rencontrées par les personnes suivies (commentaires, observations, évaluation). Dans ce cas, le fichier doit être autorisé par la CNIL (article 25-I-7°).

De même, un fichier utilisé par un bailleur pour gérer des contentieux (avec son personnel, les résidents, ses cocontractants, …) doit aussi être autorisé par la CNIL, dès lors qu'il porte sur des infractions ou des condamnations.

Pour ces deux dernières finalités (accompagnement social et gestion de contentieux), deux autorisations uniques permettent à un bailleur social, sous réserve de respecter les cadres fixés par la CNIL, de bénéficier d'une procédure d'autorisation simplifiée.

Un engagement de conformité à l'autorisation unique n° 035 permet ainsi à un bailleur social d'obtenir rapidement une autorisation pour traiter des appréciations sur des difficultés sociales dans le cadre de l'attribution, de l'adaptation et de la mutation des logements ou de la mise en place d'un suivi social.

Par ailleurs, un engagement de conformité à l'autorisation unique n° 034 permet à un bailleur social de traiter des données relatives à des infractions, condamnations ou mesures de sûreté pour gérer des précontentieux et des contentieux ou mettre en application des décisions de justice qui ont une incidence sur un lieu de résidence.

### *Les 10 questions à se poser avant de créer un fichier*

**1.** Quel est le but de ce fichier ? (à quoi va-t-il servir ?)
**2.** Est-ce légitime, notamment au regard de mes missions et des droits des personnes ?
**3.** Comment présenter cette finalité pour la rendre compréhensible par tous ?
**4.** Quelles sont les données dont j'ai forcément besoin pour atteindre l'objectif fixé ?
**5.** Jusqu'à quand ces données me seront-elles utiles (évènement butoir, durée, obligations légales ou sauvegarde d'un droit en justice) ?
**6.** Quels sont les membres de mon personnel qui ont besoin d'y accéder ?
**7.** Existe-t-il des textes m'obligeant à les conserver un certain temps ou à les communiquer à des organismes tiers ?
**8.** Comment vais-je informer les personnes concernées par mon fichier et garantir leurs droits ?
**9.** Au regard des risques et de la nature des données, quelles sont les mesures de sécurité à prévoir (mesures techniques et organisationnelles) ?
**10.** Quelle est la formalité à accomplir auprès de la CNIL (déclaration ou autorisation) ?

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

Introduit en août 2004 lors de la refonte de la loi « Informatique et Libertés », le correspondant à la protection des données personnelles (CIL) est un moyen efficace pour veiller à l'application de la loi et assurer le respect du droit à la protection des données personnelles.

Au 1er octobre 2014 environ 3.800 CIL représentant 13.400 organismes ont été désignés. Le nombre plus élevé d'organismes que de CIL désignés s'explique par le fait que la fonction peut être mutualisée entre plusieurs organismes.

La désignation d'un CIL permet un allègement des formalités préalables.

En effet, une fois le correspondant désigné, seuls les traitements soumis à autorisation ou avis préalables de la CNIL devront faire l'objet d'une formalité.

Les autres traitements n'auront plus qu'à être référencés dans une liste tenue localement par le correspondant (le registre).

## INFORMATIONS PRATIQUES

### *Le CIL*

***Pourquoi désigner un CIL ?***

*Sa désignation, qui est facultative, exonère de déclaration la plupart des fichiers. Il contribue à une meilleure application de la loi.*

***Quels avantages ?***

*Le CIL est un acteur de la sécurité juridique et technique au sein de l'organisme.*

*Son action peut prendre plusieurs formes : le conseil, la recommandation, la sensibilisation, la médiation et l'alerte en cas de dysfonctionnement.*

***Comment désigner un CIL ?***

*C'est simple, il suffit de compléter en ligne le formulaire de désignation sur le site internet de la CNIL.*

***Comment le CIL peut-il/elle être formé(e) ?***

*La CNIL propose des ateliers d'information gratuits, généralistes et thématiques, animés par ses propres experts.*

***Quelle relation avec la CNIL ?***

*La CNIL a mis en place un service spécifique pour garantir au CIL une réponse rapide et de qualité.*

*Il s'agit d'un guichet unique pour toutes les questions juridiques ou les éclairages liés à l'exercice de la fonction.*

***D'autres avantages ?***

*Le CIL est un interlocuteur privilégié de la CNIL. Ses demandes sont donc traitées en priorité.*

*Il fait partie du réseau des CIL animé par la CNIL.*

*Il participe à la réflexion liée à l'évolution de la fonction, à la création d'outils de travail, des textes juridiques …*

# FICHE N°1
# LES OUTILS DE SIMPLIFICATION DES FORMALITÉS DU PACK DE CONFORMITÉ DÉDIÉ AU LOGEMENT SOCIAL

*Pour simplifier les démarches que les bailleurs doivent accomplir auprès de la CNIL, avant de créer un fichier, trois outils de simplifications ont été élaborés au cours de l'année 2013 en concertation avec l'Union sociale pour l'habitat (USH) et des bailleurs sociaux.*

*Ces outils concernent des fichiers couramment utilisés par les bailleurs sociaux, notamment pour instruire les demandes de logements, gérer leur parc immobilier, ou instruire des précontentieux et des contentieux avec les résidents.*

*Si ces outils ont par nature une forte composante juridique, ils présentent également une dimension pédagogique, en rappelant la nécessite de respecter certaines règles juridiques et en expliquant comment y parvenir.*

*Les fiches pratiques de ce guide ont vocation à préciser et illustrer ces outils juridiques, ainsi qu'à répondre à des questions concrètes que peuvent se poser les bailleurs sociaux.*

**PRÉCISION**

Les outils du pack de conformité utilisent la notion de résident et non de locataire, puisqu'ils visent aussi bien les titulaires d'un bail d'habitation que les personnes hébergées sans bail.

Le fait qu'un outil du pack ouvre la possibilité de collecter un type de donnée ne doit pas inciter à le faire systématiquement pour tout le monde. En effet, la finalité poursuivie et la situation individuelle d'un résident doit rendre nécessaire cette collecte. En d'autres termes, la collecte d'une donnée doit être légitime et proportionnée par rapport au but recherché.

*Par exemple : ne pas collecter une pathologie quand une attitude à adopter face à un handicap est suffisante.*

## UNE NORME SIMPLIFIÉE MISE À JOUR

La norme simplifiée n° 20, adoptée en 1997 et modifiée en 2001, était devenue obsolète avec le temps. Partant de ce constat, il a été décidé de la revoir en profondeur.

Cette norme concerne aujourd'hui les fichiers et applications utilisés par les bailleurs sociaux pour :

- **enregistrer et instruire les demandes de logement social** (en accession à la propriété et en location) ;
- **assurer une gestion du patrimoine immobilier** au sens large du terme (c'est-à-dire également la gestion des logements intermédiaires, des logements foyers et des résidences sociales ou étudiantes) ;
- **mettre en place des systèmes de vidéosurveillance** respectueux des droits et libertés de chacun, et en particulier soucieux du respect de la vie privée ;
- **gérer des systèmes de contrôles d'accès** aux zones non ouvertes au public.

FICHE N°1

# LES OUTILS DE SIMPLIFICATION DES FORMALITÉS DU PACK DE CONFORMITÉ DÉDIÉ AU LOGEMENT SOCIAL

## PRÉCISION

### *La sous-finalité « gestion locative et patrimoniale » à l'initiative d'un bailleur*

Parmi les sous-finalités de la norme simplifiée n° 20, figure la gestion locative et patrimoniale des logements et de leurs accessoires.

Pour la CNIL, cela comprend notamment :

- l'établissement des baux et des états des lieux ;
- la gestion financière (facturation, encaissement, relance, recouvrement, décomptes des taxes ou charges, régularisation des charges, calcul du supplément de loyer, quittancement des loyers et relances) ;
- la gestion des réclamations, des travaux d'adaptabilité ou de réhabilitation ;
- la gestion des sinistres, des interventions et des secours (en particulier dans les immeubles de grande hauteur) ;
- la gestion des permanences téléphoniques et des extranets ;
- la gestion des bourses d'échange et des dispositifs de sous-location ;
- la gestion des anomalies d'occupation (cession ou sous-location prohibée, sous-occupation et sur-occupation) ;
- les dispositifs de médiation ou d'intermédiation locative ;
- la gestion des mandats de gérance ;
- les opérations de relogement ;
- le suivi et analyse des consommations d'énergie et d'eau, uniquement dans le cadre d'une politique de lutte contre la précarité énergétique et la maîtrise des charges et sous réserve d'une analyse des économies d'énergie prévue par un cadre réglementaire ou sur la base d'un consentement individuel ;
- les dispositifs de prévention des expulsions.

## ATTENTION

La NS 20 permet, sous certaines conditions, de traiter des données relatives à la santé des résidents. En revanche, elle ne prévoit pas la possibilité de collecter ou réaliser des appréciations sur des difficultés sociales rencontrées par des personnes.

En effet, la loi « Informatique et Libertés » prévoit que le traitement de ce type de données, en raison de son caractère sensible, doit être autorisé par la CNIL. Il n'est donc pas juridiquement possible de l'insérer dans une norme simplifiée, qui a la valeur juridique d'une simple déclaration.

Consciente que des bailleurs sociaux peuvent néanmoins avoir besoin de ce type de données dans le cadre d'une activité normale, notamment pour attribuer des logements convenant à chaque situation individuelle, la CNIL a adopté une autorisation unique qui permet aux bailleurs de traiter cette catégorie de donnée avec une formalité allégée, c'est-à-dire sur la base d'une autorisation unique.

FICHE N°1

# LES OUTILS DE SIMPLIFICATION DES FORMALITÉS DU PACK DE CONFORMITÉ DÉDIÉ AU LOGEMENT SOCIAL

## UNE AUTORISATION UNIQUE PERMETTANT DE TRAITER DES APPRÉCIATIONS SUR DES DIFFICULTÉS SOCIALES

Le pack de conformité dédié aux bailleurs sociaux comprend ainsi une autorisation unique autorisant à traiter des appréciations sur des difficultés sociales des résidents pour :

- attribuer ou adapter des logements ;
- proposer aux résidents qui le souhaitent un suivi social personnalisé.

**PRÉCISION**

Là encore, ce n'est pas parce qu'une autorisation unique prévoit la possibilité de collecter ce type de donnée qu'il faut le généraliser à tous les résidents.

## UNE AUTORISATION UNIQUE POUR GÉRER DES PRÉCONTENTIEUX ET CONTENTIEUX

Une seconde autorisation unique réservée aux bailleurs sociaux a également été élaborée par la CNIL.

Elle concerne la gestion du précontentieux et du contentieux par les bailleurs sociaux, notamment en matière :

- de trouble anormal de voisinage ;
- de recouvrement des impayés ;
- d'expulsion locative ;
- d'atteintes au patrimoine immobilier ou aux personnes.

Cette autorisation unique comporte également une sous finalité permettant aux bailleurs de mettre concrètement en application des décisions de justice, lorsqu'elles ont une incidence sur un lieu de résidence (ex : jugement d'éloignement d'un résident violent).

En effet, il semble pertinent qu'un bailleur ait connaissance de cette information à l'initiative de la personne concernée, notamment pour ne pas reloger la personne éloignée trop près.

En revanche, la raison à l'origine de la condamnation ne doit pas être renseignée dans le système d'information d'un bailleur social. Cette information ne présente en effet pas d'intérêt dans le cadre d'un relogement.

# FICHE N°2
# PERSONNES HABILITÉES, SOUS-TRAITANTS, DESTINATAIRES DES DONNÉES ET TIERS AUTORISÉS

*L'article 34 de la loi « Informatique et Libertés » impose qu'un responsable de traitement, au regard de la nature des données et des risques présentés par chaque fichier, prenne toutes les précautions utiles pour préserver la sécurité des données à caractère personnel dont il est responsable et, notamment, qu'il empêche les tiers non autorisés à y accéder.*

*Un bailleur social, en qualité de responsable de traitement, doit ainsi garantir la confidentialité des données relatives à son personnel ou aux résidents.*

*Il doit dès lors prendre un certain nombre de précautions lorsqu'il envisage de communiquer ou de rendre accessibles ces données.*

**RAPPEL**

L'article 3-II de la loi « Informatique et Libertés » définit un destinataire de données à caractère personnel comme étant « toute personne habilitée à recevoir communication de ces données autres que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données ».

Cet article précise que « ***les autorités légalement habilitées***, *dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander à un responsable de traitement la communication de données à caractère personnel* ***ne constituent pas des destinataires*** ».

## 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

FICHE N°2

# PERSONNES HABILITÉES, SOUS-TRAITANTS, DESTINATAIRES DES DONNÉES ET TIERS AUTORISÉS

toutefois à un certaine nombre de règles organisationnelles et techniques.

Le responsable de traitement doit en effet veiller à ce que l'accès aux données qu'il détient ne soit rendu possible qu'aux seuls employés habilités à en connaitre au regard de leurs attributions.

En d'autres termes, les données qu'un employé peut consulter et traiter pour son activité professionnelle doivent présenter un intérêt légitime par rapport à ses missions, et être proportionnées à ces dernières.

Il est dès lors indispensable de mettre en place une politique d'habilitation permettant une gestion efficace des droits d'accès aux données.

Cette politique dépend nécessairement de l'organisation de l'entité en cause, ce qui explique qu'une catégorie d'employés habilités dans une structure à accéder à des données peut ne pas avoir besoin d'y accéder dans une autre.

À titre illustratif, les gardiens d'immeuble ont très souvent des tâches différentes, ce qui se traduit dans la nature des données auxquelles ils peuvent légitimement accéder.

Certains d'entre eux participent par exemple au recouvrement des loyers et ont donc besoin d'avoir accès aux données en rapport avec cette mission particulière (montant à payer, date d'échéance, éventuelles échelonnement d'une dette locative, ...). Le responsable de traitement doit toutefois veiller à ce que les gardiens impliqués dans le recouvrement des loyers n'accèdent pas à des données sans intérêt pour l'exercice de cette mission, par exemple le motif associé à un échelonnement d'une dette locative ou la situation financière des résidents.

Les employés habilités à accéder à des données à caractère personnel n'étant pas des destinataires, ils n'ont pas être mentionnés à ce titre dans un dossier de formalité préalable adressé à la CNIL (déclaration ou demande d'autorisation). Une autre conséquence de cette distinction tient au fait que les personnes concernées par le traitement (résidents, employés, fournisseurs...) n'ont pas à être spécifiquement informées de la communication de donnés les concernant aux employés habilités à les traiter. En effet, l'article 32-5° de la loi « Informatique et Libertés » prévoit uniquement d'informer les personnes concernées par un fichier au sujet des « destinataires ou catégories de destinataires des données ». Si cette précision n'est pas obligatoire, elle n'est toutefois pas interdite et peut apparaître utile ne serait-ce que de façon générique en précisant aux résidents que les employés habilités peuvent accéder à leurs données dans le cadre de leur activité professionnelle, ce qui permet d'ailleurs de formaliser une politique d'habilitation.

## L'ACCÈS AUX DONNÉES PAR LES SOUS-TRAITANTS

Un sous-traitant, défini par l'article 35 de la loi « Informatique et Libertés comme « toute personne traitant des données à caractère personnel pour le compte d'un responsable de traitement », n'est pas un destinataire au sens de cette loi.

À l'image des règles applicables aux employés du responsable de traitement, un sous-traitant ne doit accéder qu'aux seules données indispensables à l'exercice de la prestation qui lui est confiée.

Un prestataire chargé d'installer ou de réparer un dispositif permettant de filtrer les accès à des zones particulières (interphone, digiphone, badges nominatifs, ...) ne doit ainsi avoir accès qu'à un nombre limité de données personnelles. Par exemple, il n'est pas possible de lui communiquer les numéros de téléphone des résidents, dès lors qu'il n'a pas besoin de les contacter pour prendre rendez-vous et que le dispositif n'est pas relié aux lignes téléphoniques.

De façon générale, un responsable de traitement doit transmettre les données à ses sous-traitants de façon sécurisée et leur imposer de mettre en place des mesures per-

FICHE N°2

# PERSONNES HABILITÉES, SOUS-TRAITANTS, DESTINATAIRES DES DONNÉES ET TIERS AUTORISÉS

mettant de garantir la sécurité et la confidentialité des données confiées.

La loi « Informatique et Libertés » (article 35) prévoit à ce titre que le contrat qui lie un responsable de traitement à un sous-traitant doit notamment mentionner les obligations de ce dernier en matière de protection des données. Prévoir que le prestataire doit agir que sur instruction de son donneur d'ordre, ce qui lui interdit notamment de communiquer à des tiers les données qui lui sont remises.

Parmi ces obligations, il doit également être prévu que les données confiées au sous-traitant, une fois sa mission terminée, doivent être détruites ou rendues au responsable de traitement.

Les sous-traitants n'étant pas des destinataires au sens de la loi « Informatique et Libertés », ils n'ont pas à être mentionnés à ce titre dans un dossier de formalité préalable adressé à la CNIL (déclaration ou demande d'autorisation).

Par ailleurs, de la même façon que pour les employés habilités à traiter des données, il n'est pas obligatoire que les personnes concernées (résidents, employés…) soient spécifiquement informées de la communication de donnés les concernant à un sous-traitant. Cette information peut toutefois leur être délivrée, ce qui évitera par exemple que des résidents soient surpris d'être contactés par un organisme disposant de données à leur sujet sans avoir été préalablement en contact directement avec lui.

## LA COMMUNICATION DE DONNÉES À UN DESTINATAIRE

La loi « Informatique et Libertés » définit un destinataire comme toute personne habilitée à recevoir communication de données autre que la personne concernée, le responsable du traitement, les sous-traitants et les personnes qui en raison de leurs fonctions sont chargées de traiter les données.

Au sens strict du terme, un destinataire est ainsi une personne ou un organisme externe auquel un bailleur social transmet des données, en dehors du cas spécifique des sous-traitants.

Il peut s'agir d'une communication de données à l'initiative du bailleur ou, au contraire, consécutive à une demande d'un organisme externe que le bailleur estime légitime.

La communication de données à un destinataire, par exemple les coordonnées des résidents pour leur proposer des offres commerciales, telles que la fourniture d'un accès à internet, des services à la personne ou un l'achat d'un bien immobilier, obéit à un certain nombre de règles qu'il convient de préciser.

Tout d'abord, le responsable de traitement doit s'interroger sur la finalité de la transmission pour s'assurer de sa pertinence et de sa légitimité. À cette occasion, il doit notamment s'assurer que les données transmises ne feront pas l'objet d'un traitement ultérieur contraire à la finalité de la transmission, au besoin par la conclusion d'un contrat avec le destinataire.

Le responsable de traitement doit ensuite vérifier que les données communiquées sont adéquates, pertinentes et non excessives au regard la finalité poursuivie, d'une part, et qu'elles ne seront pas conservées au-delà du temps nécessaires à l'accomplissement de cette dernière, d'autre part.

Avant de procéder à la communication des données, le responsable du traitement doit enfin en informer les personnes concernées et les mettre en mesure de s'y opposer.

La communication des données doit être effectuée selon des modalités permettant de s'assurer de leur confidentialité, étant précisé que le niveau de sécurité dépend de la nature des données et des risques supposés. En d'autres termes, plus les données sont sensibles, plus les mesures de sécurité devront être robustes.

S'agissant de l'exercice des droits des personnes, la loi « Informatique et Libertés » (article 40) prévoit, par ailleurs, qu'un responsable de traitement qui a communiqué des données à un destinataire doit lui indiquer les opérations de rectification ou de suppression

FICHE N°2

# PERSONNES HABILITÉES, SOUS-TRAITANTS, DESTINATAIRES DES DONNÉES ET TIERS AUTORISÉS

effectuées sur les données, pour que le destinataire adopte les mêmes mesures.

Le responsable du traitement initial, de la même façon qu'il doit le faire avec un sous-traitant, doit aussi vérifier que le destinataire des données, au regard de la nature des données et des risques présentés par le traitement, mettra en œuvre les mesures de sécurité adéquates pour garantir la confidentialité des données transmises.

Enfin, les formalités déjà effectuées auprès de la CNIL devront être modifiées pour y mentionner le nouveau destinataire des données.

Le responsable initial des données devra, par ailleurs, attirer l'attention du destinataire sur le fait qu'il lui appartient d'accomplir auprès de la CNIL les formalités prévues par la loi (déclaration ou demande d'autorisation).

## LA COMMUNICATION DE DONNÉES À UN TIERS AUTORISÉ

Les tiers autorisés sont les organismes autorisés par une disposition législative ou réglementaire, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à obtenir d'un responsable de traitement la communication de données à caractère personnel.

Lorsqu'un bailleur social est confronté à une demande de communication venant d'un tiers s'appuyant sur un texte, il doit s'assurer que la disposition avancée est en vigueur, et qu'elle prévoit effectivement un droit de communication au bénéfice du demandeur.

Le bailleur sollicité doit, par la suite, veiller à ne transmettre que les données prévues par le texte ou, en cas d'imprécision de ce dernier, les seules données qui lui apparaissent strictement nécessaires pour atteindre le but recherché.

La communication des données devra être réalisée selon des modalités permettant de s'assurer de leur sécurité, en adaptant la mesure retenue à la nature des données et aux risques en présence.

Les tiers autorisés, au même titre que les employés habilités du bailleur et les sous-traitants, n'ont pas à être mentionnés dans un dossier de formalité préalable adressé à la CNIL puisqu'ils ne sont pas considérés comme des destinataires (déclaration ou demande d'autorisation).

Par ailleurs, il n'est pas non plus obligatoire d'informer les personnes concernées des transmissions de données à leur profit.

Informer les personnes concernées par un fichier (résidents, employés, ...) sur le fait que des données les concernant sont susceptibles d'être communiquées à des tiers légalement habilités à en connaitre peut toutefois apparaître utile, y compris si l'information délivrée reste générale en se limitant à indiquer cette possibilité (c'est-à-dire sans lister l'intégralité des tiers autorisés).

FICHE N°2

# PERSONNES HABILITÉES, SOUS-TRAITANTS, DESTINATAIRES DES DONNÉES ET TIERS AUTORISÉS

## Liste non exhaustive de tiers autorisés à obtenir la communication de données auprès d'un bailleur social

| Données concernées | Organisme autorisé | Fondement légal |
|---|---|---|
| Demandes locatives | Commission d'attribution | *articles L. 441-2 et R. 441-9 du code de la construction et de l'habitation* |
| | Réservataires de logements | *articles L. 441-1, L. 441-2-1 et R. 441-5 du code de la construction et de l'habitation* |
| | Commission de coordination de l'accord collectif intercommunal | *article L. 441-1-1 du code de la construction et de l'habitation* |
| | Commission de médiation dite « DALO » | *article L. 441-2-3-1 du code de la construction et de l'habitation* |
| | Mission interministérielle d'inspection du logement social | *articles L. 451-1 et suivants du code de la construction et de l'habitation* |
| | Système national d'enregistrement et dispositifs de gestion partagée des demandes | *article R. 441-2-6 du code de la construction et de l'habitation* |
| | Départements, communes, établissements publics de coopération intercommunale, service commun d'enregistrement et service intégré d'accueil et d'intégration compétents assurant le service d'enregistrement des demandes (délibération prise à cet effet) | *article L. 441-2-1 du code de la construction et de l'habitation* |
| | Service de l'État ou du département assurant le secrétariat des instances locales du plan départemental d'action pour le logement et l'hébergement des personnes défavorisées | *article 2 et suivants de la loi n° 90-449 du 31 mai 1990 modifiée visant à la mise en œuvre du droit au logement et article R. 441-2-6 du code de la construction et de l'habitation* |
| | Services instructeurs des dossiers d'agrément (procédure de location-accession à la propriété immobilière) | *articles R. 331-76-5-1 et suivants du code de la construction et de l'habitation* |
| | Mission interministérielle d'inspection du logement social | *articles L. 451-1 et suivants du code de la construction et de l'habitation* |

FICHE N°2

# PERSONNES HABILITÉES, SOUS-TRAITANTS, DESTINATAIRES DES DONNÉES ET TIERS AUTORISÉS

| | | |
|---|---|---|
| **Gestion du patrimoine** | Organisme payeur d'aides au logement | *article L.351-1 code de la construction et de l'habitation, article L. 331-1 et L. 542-1 du code de la sécurité sociale* |
| | Caisses d'allocation familiales et Mutualité sociale agricole | *article L. 351-14 du code de la construction et de l'habitation* |
| | Commission de coordination des actions de prévention des expulsions | article 7-2 de la loi n° 90-449 du 31 mai 1990 visant la mise en œuvre du droit au logement et décret n° 2008-187 du 26 février 2008 ; article de la 24 loi n° 89-462 du 6 juillet 1989 tendant à améliorer les rapports locatifs et portant modification de la loi n° 86-1290 du 23 décembre 1986 |
| | Fonds de solidarité pour le logement | article 6 de la loi n° 90-449 du 31 mai 1990 visant la mise en œuvre du droit au logement |
| | Organisme participant à l'élaboration et à la mise en œuvre du plan départemental d'action pour le logement et l'hébergement des personnes défavorisées | loi n° 90-449 du 31 mai 1990 visant la mise en œuvre du droit au logement |
| | Associations ou structures gestionnaires de logements sous-loués à titre transitoire à une personne ou à une famille éprouvant des difficultés particulières | article L. 442-8-3 du code de la construction et de l'habitation |
| | Fournisseur d'énergie pour les clients éligibles au tarif social de solidarité ou au tarif de première nécessité | article L. 445-5 du code de l'énergie |
| | Services du Trésor public (recouvrement des loyers des organismes publics) | article L. 1617-5 du code général des collectivités territoriales |
| | Commission de surendettement | article L. 331-1 du code de la consommation |
| | Commission de médiation dite « DALO » | article L. 441-2-3 du code de la construction et de l'habitation |
| | Services des mairies et collectivités locales en charge des affaires économiques pour obtenir l'avis de la commune préalablement à la location de locaux d'habitation situé en rez-de-chaussée en vue d'y exercer une activité économique | article L. 443-11 du code de la construction et de l'habitation |

# FICHE N°3
# DURÉE DE CONSERVATION ET ARCHIVAGE DES DONNÉES

*Les bailleurs sociaux sont amenés à collecter, dans le cadre de leurs diverses activités, de nombreuses données sur le compte des demandeurs de logement social, des résidents ou des personnes intervenant sur le parc immobilier.*

*Combien de temps les données peuvent-elles être conservées ? Est-il possible d'archiver certaines d'entre-elles ? Sous quelles conditions ?*

## UNE DURÉE DE CONSERVATION LIMITÉE EN BASE ACTIVE

La loi « Informatique et Libertés » (article 6-5°) prévoit que les données à caractère personnel, c'est-à-dire celles permettant d'identifier directement ou indirectement une personne physique, doivent être conservées uniquement le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte.

En dehors des cas dans lesquels il existe une obligation permettant un archivage (Cf. infra), les données qui ne présentent plus d'intérêt, parce que la finalité poursuivie a été atteinte, doivent être supprimées sans délai par le responsable de traitement. En cas de procédure de suppression automatique, le responsable de traitement doit s'assurer que les données sont effectivement supprimées.

La durée de conservation en base active est variable et dépend de la nature des données et des finalités poursuivies.

De manière générale, les données collectées par un bailleur dans le cadre d'une demande de logement social doivent être supprimées à compter de la radiation de la demande ou en cas d'attribution d'un logement. Tel est le cas, par exemple, du périmètre géographique souhaité qui ne semble présenter d'intérêt que pour attribuer un logement compatible avec le(s) souhait(s) du demandeur. De la même manière, les pièces justificatives demandées pour instruire une demande ne présentent plus d'intérêt une fois le logement attribué.

En revanche, lorsque des données recueillies dans le cadre d'une demande de logement peuvent encore présenter un intérêt pour de la gestion locative (nom des occupants, coordonnées, ressources déclarées, …), elles peuvent être conservées le temps nécessaire à cette seconde finalité, sous réserve d'en avoir informé les personnes concernées. Cette possibilité de conservation supplémentaire cesse toutefois quand la seconde finalité est atteinte.

Si un demandeur souhaite que des données le concernant soient supprimées avant d'avoir obtenu un logement, cette demande doit être immédiatement prise en compte. Le dossier correspond sera logiquement supprimé et aucun logement ne pourra être attribué.

Lorsqu'une demande d'accession à la propriété est satisfaite, les données relatives à cette demande doivent être supprimées à compter du paiement complet du logement ou, le cas échéant, à l'issue de la période de sécurisation de la transaction.

S'agissant des données collectées par le gestionnaire d'un ensemble immobilier sur le compte des résidents, elles doivent être supprimées de la base active à compter du règlement du solde de tout compte des intéressés.

FICHE N°3

# DURÉE DE CONSERVATION ET ARCHIVAGE DES DONNÉES

Les données recueillies dans le cadre d'une intervention dans un logement, ou sur les parties communes, doivent quant à elles être supprimées de la base active lorsque l'opération en question est achevée, notamment à compter de la date de réception des travaux. A compter de cet évènement, puisque les travaux sont réalisés, la finalité est atteinte et les données précédemment collectées doivent être supprimées.

S'agissant des systèmes de vidéoprotection, les données collectées ne doivent pas être conservées plus d'un mois. Lorsqu'un incident est constaté par ce bais, les données correspondantes doivent être extraites du dispositif et conservées sur un support distinct jusqu'à la régularisation de la situation.

## LA POSSIBILITÉ D'UN ARCHIVAGE

Parmi les nombreuses données à caractère personnel qu'un bailleur social est amené à collecter au fil de son activité, certaines d'entre elles, à l'issue de leur conservation en base active, peuvent faire l'objet d'un archivage lorsqu'elles présentent encore un intérêt. Par exemple, pour satisfaire à une obligation à sa charge ou se prémunir contre un éventuel contentieux.

Dans certaines hypothèses, l'archivage peut même être obligatoire. Un bailleur social peut ainsi archiver des données concernant d'anciens résidents pour être en mesure de satisfaire à un contrôle de la Mission interministérielle d'inspection du logement social (MIILOS).

Il peut également conserver des données relatives à des demandes ou des attributions de logements pour mettre en place un contrôle interne quant au respect des règles d'attribution, justifier auprès de réservataires de la bonne utilisation des droits de réservation, ou réaliser des études concernant les demandes et attributions de logements sociaux.

De la même façon, des données correspondantes à des parcours résidentiels peuvent être archivées aux fins de transmissions aux Commissions de médiation dites « DALO ».

### Un archivage sélectif

Le responsable de traitement doit veiller à archiver les seules données permettant de respecter l'obligation prévue par le texte à l'origine de l'archivage ou, lorsque c'est la raison de l'archivage, pour faire valoir un droit en justice. Il doit, dès lors, opérer un tri parmi la totalité des données collectées pour ne garder que les seules données indispensables.

**ATTENTION**

Lorsqu'une personne exerce son droit d'accès, il doit obtenir la communication de l'intégralité des données qui le concernent, qu'elles soient stockées en base active ou archivées.

### Un archivage limité dans le temps

Les données nécessaires pour répondre à une obligation légale ou réglementaire peuvent être archivées le temps correspondant à l'accomplissement de l'obligation en cause. Les données archivées doivent être supprimées lorsque la raison justifiant leur archivage n'a plus raison d'être.

Les données archivées en prévision d'un éventuel contrôle de la MIILOS doivent, par exemple, être définitivement supprimées lorsque le contrôle ne peut plus être légalement opéré.

De la même façon, des données archivées pour faire valoir un droit en justice doivent être supprimées lorsque cette action est prescrite.

FICHE N°3

# DURÉE DE CONSERVATION ET ARCHIVAGE DES DONNÉES

S'agissant d'un archivage mis en place pour exercer un contrôle interne quant aux respect des règles d'attributions des logements ou pour rendre compte de son activité auprès d'organismes externes, tels que les réservataires des logements, une durée d'archivage de 18 mois apparait justifiée, en ce qu'elle permet de vérifier l'activité d'un exercice annuel jusqu'au 30 juin de l'exercice comptable suivant.

Une telle durée d'archivage de 18 mois peut également être justifiée par le suivi des engagements pris par un organisme d'habitation à loyer modéré en faveur de personnes en difficultés, dans les accords collectifs visés à l'article L. 441-1-1 du code de la construction et de l'habitation et conclus sur le territoire d'un établissement publics de coopération intercommunale compétent en matière d'habitat.

**PRÉCISION**

Seules les données présentant un intérêt historique, scientifique ou statistique peuvent être conservées sans limitation de durée. Dans ce cas, on parle d'archivage définitif. En tout état de cause, il est obligatoire de sélectionner les seules données pouvant relever de cette exception.

## Un mode d'archivage libre

Le choix du mode d'archivage est laissé à l'appréciation du responsable de traitement. Des données peuvent ainsi être archivées :

- dans une base d'archive spécifique, distincte de la base active, avec des accès restreints aux seules personnes ayant un intérêt à en connaitre en raison de leurs fonctions (par exemple, le service du contentieux) ;
- ou dans la base active, à condition de procéder à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) pour les rendre inaccessibles aux personnes n'ayant plus d'intérêt à les traiter.

S'agissant des archives définitives (c'est-à-dire les seules données présentant un intérêt historique, scientifique ou statistique), il est recommandé de les conserver sur un support indépendant, non accessible par les systèmes de production, n'autorisant qu'un accès distinct, ponctuel et précisément motivé auprès d'un service spécifique seul habilité à les consulter (par exemple, la direction des archives lorsqu'elle existe).

**PRÉCISION**

Quel que soit le type d'archive, il faut prévoir une traçabilité des consultations des données archivées.

## Un archivage sécurisé

Des mesures techniques et organisationnelles appropriées doivent être prévues pour protéger les données archivées (destruction, perte, altération, diffusion ou accès non autorisés...).

Ces mesures doivent assurer un niveau de sécurité approprié au regard des risques et de la nature des données.

Lorsque l'archivage est confié à un sous-traitant, le responsable du traitement doit s'assurer que son prestataire présente des garanties suffisantes en matière de sécurité et la confidentialité des données qui lui sont confiées.

# FICHE N°4
# LA VIDÉOSURVEILLANCE ET LA VIDÉOPROTECTION DANS LES ENSEMBLES IMMOBILIERS À CARACTÈRE SOCIAL

*Des dispositifs de vidéosurveillance sont régulièrement installés par les bailleurs sociaux pour lutter contre les vols ou les dégradations, par exemple dans les parkings ou les halls d'entrée.*

*Ces dispositifs doivent respecter certaines règles, afin de ne pas porter atteinte à la vie privée des locataires et de leurs visiteurs.*

*Quelles sont ces règles ? Quelles précautions prendre ? Quels sont les droits des personnes filmées ?*

## L'INSTALLATION DE CAMÉRAS DE VIDÉOSURVEILLANCE *dans les lieux non ouverts au public*

Les bailleurs ont l'obligation de garantir la sécurité et la tranquillité résidentielle, notamment en installant et en entretenant :

- un éclairage assurant une bonne visibilité de l'entrée des immeubles et de leurs parties communes, notamment des parkings ;
- des systèmes permettant de limiter, aux seuls résidents et personnes autorisées par ces derniers ou habilitées par le bailleur, l'accès aux parties communes des immeubles, aux caves et aux parkings.

Des caméras peuvent également être installées dans les lieux non ouverts au public afin de participer au respect de cette obligation, lorsqu'elles s'avèrent nécessaires au regard des difficultés rencontrées. Dans ce cas, l'installation des caméras doit être déclarée à la CNIL (*Cf. infra*)

Elles peuvent filmer les espaces communs à des fins de sécurité des biens et des personnes.

Il est, par exemple, possible d'installer des caméras à la suite de vols ou de dégradations de véhicules dans le parking souterrain d'un immeuble, à titre dissuasif ou pour identifier les auteurs. Des caméras peuvent également être installées dans le hall d'entrée pour éviter les tags ou la dégradation de boîtes aux lettres.

Les caméras peuvent uniquement filmer les espaces communs (parking, local à vélos ou poussettes, hall d'entrée, portes d'ascenseur, cour…). Elles ne doivent pas filmer

l'intérieur des logements, les portes des appartements, les fenêtres, les balcons ou encore les terrasses des habitants. Les dispositifs permettant de visualiser des images, en direct ou enregistrées, ne doivent pas être librement accessibles à l'ensemble des habitants. Seules les personnes habilités doivent pouvoir visualiser les images.

L'écran de contrôle doit être orienté de façon à ce que les images ne soient pas visibles par un tiers, par exemple depuis l'extérieur de la loge du gardien à travers la fenêtre. De même, il convient de prévoir un verrouillage automatique du poste de visualisation, de façon à ce que les images ne puissent être vues si le gardien s'absente de sa loge en ne verrouillant pas son accès.

Par principe, les images doivent être consultées par les employés habilités uniquement à la suite d'un incident (vandalisme, dégradation, agression…). Un officier de

FICHE N°4

# LA VIDÉOSURVEILLANCE ET LA VIDÉOPROTECTION DANS LES ENSEMBLES IMMOBILIERS À CARACTÈRE SOCIAL

police judiciaire (OPJ) ou un magistrat peut toutefois, par réquisition judiciaire, obtenir lecture ou copie de telles images.

Les caméras ne doivent pas servir à « surveiller » en temps réel les allées et venues des résidents, des visiteurs ou des employés.

Les gardiens, lorsqu'ils ont accès aux images, doivent être particulièrement sensibilisés à cette question, par exemple en ayant bénéficié d'une formation spécifique.

**ATTENTION**

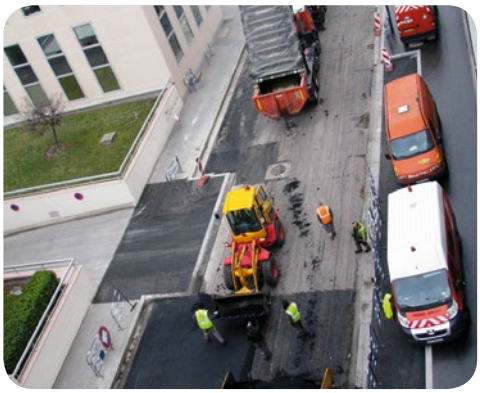
Les images ne peuvent pas être utilisées pour surveiller les employés.

Il est également interdit d'utiliser un système de reconnaissance faciale.

## L'INSTALLATION DE CAMÉRAS DE VIDÉOPROTECTION *dans les lieux ouverts au public*

Par principe, seules les autorités publiques peuvent filmer la voie publique (c'est-à-dire les rues).

Les bailleurs sociaux peuvent filmer les espaces non ouverts au public relevant de leur patrimoine (parking, hall d'immeuble, etc.) tel que précisé ci-dessus, ainsi que les abords immédiats des bâtiments et des installations qui leur appartiennent (façade extérieure, passages ouverts au public en bas des immeubles, etc.). Ils ne peuvent en revanche filmer spécifiquement les rues.



Un dispositif filmant un espace ouvert au public doit être autorisé par l'autorité préfectorale (*Cf. infra*).

De la même façon que pour les dispositifs de vidéosurveillance, les caméras ne doivent pas filmer l'intérieur des logements, les portes des appartements, les fenêtres, les balcons ou encore les terrasses des habitants. Par exemple, des procédés de masquage irréversible de ces zones doivent être mis en œuvre.

Seules les personnes habilitées par l'autorisation préfectorale peuvent visionner les images enregistrées. Elles doivent être particulièrement formées et sensibilisées aux règles de mise en œuvre d'un système de vidéoprotection.

**PRÉCISION**

La CNIL est compétente pour contrôler le respect des conditions de mise en œuvre des dispositifs de vidéosurveillance et de vidéoprotection.

FICHE N°4

# LA VIDÉOSURVEILLANCE ET LA VIDÉOPROTECTION DANS LES ENSEMBLES IMMOBILIERS À CARACTÈRE SOCIAL

## L'ACCÈS AUX IMAGES EN TEMPS RÉEL PAR LES FORCES DE L'ORDRE

Lors de circonstances faisant redouter la commission des atteintes aux biens ou aux personnes, les gestionnaires d'immeubles peuvent transmettre, de manière occasionnelle et en temps réel, les images enregistrées aux services de police et de gendarmerie (article L. 126-1-1 du code de la construction et de l'habitation).

**Ce type de transmission doit être autorisé par une décision de la majorité des copropriétaires ou, dans les ensembles immobiliers à caractère social, par une décision du gestionnaire.**

Par ailleurs, une convention doit être conclue entre le Préfet et le gestionnaire de l'immeuble. Lorsque la convention a pour objet de permettre la transmission des images aux services de police municipale, elle doit en outre être signée par le maire. Cette convention doit préciser les conditions et les modalités du transfert des images et être transmise à la Commission départementale de vidéoprotection, afin qu'elle apprécie les garanties prévues et puisse demander, le cas échéant, leur renforcement au Préfet.

La transmission des images doit être strictement limitée au temps nécessaire à l'intervention des services de police ou de gendarmerie.

L'existence de ce système de vidéosurveillance et la possibilité de transmission des images aux forces de l'ordre doivent être affichées sur place.

En tout état de cause, les images transmises aux forces de l'ordre ne peuvent en aucun cas porter sur l'entrée des habitations privées ou sur la voie publique.

*La transmission d'images en temps réel aux forces de l'ordre doit faire l'objet d'une déclaration normale auprès de la CNIL. À cette occasion, il convient de joindre une copie de la convention conclue en application du code de la construction et de l'habitation, ainsi que de l'avis de la Commission départementale de vidéoprotection.*

## LA DURÉE DE CONSERVATION DES IMAGES

En règle générale, conserver les images quelques jours suffit à effectuer les vérifications nécessaires en cas d'incident et permet d'enclencher d'éventuelles procédures. Si de telles procédures sont engagées, les images peuvent alors être extraites du dispositif (après consignation de cette opération dans un cahier spécifique) et conservées pour la durée de la procédure.

Les images issues des dispositifs de vidéosurveillance ne doivent pas être conservées pendant plus d'un mois.

Lorsque c'est techniquement possible, une durée maximale de conservation des images doit être paramétrée dans le système. La durée de conservation ne doit pas être fixée en fonction de la seule capacité de stockage, c'est-à-dire que les images ne doivent pas être supprimées lorsque la capacité maximale de stockage est atteinte.

FICHE N°4

# LA VIDÉOSURVEILLANCE ET LA VIDÉOPROTECTION DANS LES ENSEMBLES IMMOBILIERS À CARACTÈRE SOCIAL

## LES DROITS DES PERSONNES FILMÉES

Les personnes concernées par un système d'enregistrement vidéo doivent être informées, par un panneau affiché de façon visible, de l'existence du dispositif, du nom du responsable ainsi que des modalités concrètes d'exercice de leur droit d'accès aux enregistrements visuels les concernant.


S'agissant du droit d'accès, en application de l'article 39 de la loi « Informatique et Libertés », toute personne physique justifiant de son identité peut accéder aux enregistrements la concernant. Une copie des données la concernant doit lui être délivrée à sa demande.

Le responsable de traitement peut exiger qu'une telle demande soit effectuée par écrit et demander la production d'un justificatif d'identité. Il peut également subordonner la délivrance d'une copie au paiement d'une somme qui ne peut excéder le coût de la reproduction. En cas de facturation, il doit attester du paiement de la somme perçue.

**ATTENTION**

La communication des enregistrements doit préserver la protection des données des tiers. Il faut donc flouter ces derniers pour les rendre non identifiables ou couper certains passages des enregistrements lorsque cela est possible.

La loi prévoit que le responsable de traitement ne peut s'opposer qu'aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique (article 39-II). En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable de traitement.

## LES FORMALITÉS À ACCOMPLIR

### Auprès de la CNIL

*Pour les dispositifs dits de vidéosurveillance, c'est-à-dire filmant les lieux non ouverts au public :*

Si les caméras filment des lieux uniquement accessibles à des personnes autorisées (par exemple, un hall d'entrée lorsque l'accès à celui-ci s'effectue à l'aide d'une clé détenue uniquement par les occupants de l'immeuble) et permettent l'enregistrement des images, le dispositif doit être déclaré à la CNIL, car les lieux sont considérés comme non ouverts au public.

La norme simplifiée n° 20 prévoit une sous-finalité relative aux dispositifs de vidéosurveillance. Si le système est conforme en tout point au cadre fixé par cette norme simplifiée, un engagement de conformité suffit pour accomplir la déclaration correspondante. À défaut, il convient d'adresser à la CNIL une déclaration normale.

### Auprès de la préfecture

*Pour les dispositifs dits de vidéoprotection, c'est-à-dire filmant les lieux ouverts au public :*

Si les caméras filment un lieu accessible à toute personne (par exemple un hall d'en-

FICHE N°4

# LA VIDÉOSURVEILLANCE ET LA VIDÉOPROTECTION DANS LES ENSEMBLES IMMOBILIERS À CARACTÈRE SOCIAL

trée sans digicode ni interphone), le dispositif doit faire l'objet d'une demande d'autorisation auprès du préfet du département (le préfet de police à Paris), car les lieux sont considérés comme ouverts au public.

Le Préfet rendra sa décision, après l'avis d'une commission départementale présidée par un magistrat. L'autorisation est valable cinq ans et renouvelable.

Le formulaire peut être retiré auprès des services de la préfecture du département ou téléchargé sur le site internet du ministère de l'Intérieur. Il peut également être rempli en ligne sur le site : https://www.televideoprotection.interieur.gouv.fr

La demande d'autorisation doit être déposée par l'autorité décidant de la mise en œuvre du dispositif, éventuellement accompagnée dans cette procédure par son prestataire technique.

## LES TEXTES DE RÉFÉRENCE

**La loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés**, lorsque les caméras filment des lieux non ouverts au public (vidéosurveillance).

- Le code de la sécurité intérieure, lorsque les caméras filment des lieux ouverts au public (vidéoprotection) :
  - **Articles L223-1** et suivants (lutte contre le terrorisme)
  - **Articles L251-1** et suivants.
- Le code de la construction et de l'habitation : **Article L. 126-1-1** (accès aux images en temps réel par les services de maintien de l'ordre)
- Le code civil : **Article 9** (protection de la vie privée)
- Le code pénal :
  - **Article 226-1** (enregistrement de l'image d'une personne à son insu dans un lieu privé)
  - **Article 226-16** (non déclaration auprès de la CNIL)
  - **Article 226-18** (collecte déloyale ou illicite)
  - **Article 226-20** (durée de conservation excessive)
  - **Article 226-21** (détournement de la finalité du dispositif)
  - **Article R625-10** (absence d'information des personnes)

### POUR ALLER PLUS LOIN

**http://www.interieur.gouv.fr/Videoprotection/Documentation/Videoprotection-et-logement-social/Logement-social**

# FICHE N°5
# L'UTILISATION DES CHAMPS LIBRES ET ZONES DE COMMENTAIRES

*Les logiciels utilisés par les bailleurs sociaux proposent fréquemment d'utiliser des champs à remplir librement, parfois appelés « zones commentaires » ou « bloc-notes ». Ces champs libres permettent d'assurer le suivi d'un dossier ou de personnaliser une relation.*

*S'il n'est pas interdit par principe d'y recourir, des règles doivent toutefois encadrer leur utilisation pour éviter que ces espaces puissent porter atteinte aux droits des personnes concernées, par exemple en ayant pour effet de les priver d'une prestation, ou simplement en raison de la présence de commentaires désobligeants, discriminants, voire injurieux.*

*La présente fiche a pour objet de rappeler du secteur du logement social les règles à respecter et les bonnes pratiques à adopter.*

*La meilleure des précautions étant de garder à l'esprit que les résidents peuvent, à tout moment et sur simple demande, accéder au contenu des zones de commentaires en exerçant leur droit d'accès prévu par l'article 39 de la loi « Informatique et Libertés ».*

## LIMITER L'UTILISATION DES CHAMPS LIBRES AU PROFIT DE CASES À COCHER OU DE MENUS DÉROULANTS DÉCRIVANT DES SITUATIONS OBJECTIVES PRÉ-DÉDIFINIES

Les risques de dérives liées à l'utilisation de champs libres doivent amener le responsable de traitement à s'interroger sur l'opportunité de la mise en place de ce type d'outil, notamment au regard des bénéfices attendus.

En effet, ce type d'espace est en général utilisé pour personnaliser une relation ou assurer son suivi, mais n'est pas destiné à être utilisé comme un « outil métier » pour gérer au quotidien des dossiers administratifs.

Dans une démarche globale de mise en conformité avec la loi « Informatique et Libertés », un responsable de traitement doit ainsi veiller à ce que des zones de commentaires ne soient utilisées que dans les cas où des outils simples, tels que des cases à cocher ou des menus déroulants, ne permettraient pas d'atteindre le même objectif.

En décrivant des situations objectives ou en renvoyant à des catégories neutres, de tels outils permettent d'atteindre le même but que des zones de commentaires, en s'assurant de l'absence de commentaires excessifs.

La mise en place d'outils alternatifs aux zones de commentaire évitera ainsi au responsable de traitement d'être sanctionné, à l'occasion d'un contrôle de la CNIL comme cela a pu être le cas par le passé, en raison de la découverte de commentaires tels que : « *séropositif* », « *cancer* », « *alzheimer* », « *violence dans le travail notamment harcèlement sexuel* », « *vit ailleurs accusé de viol et a gagné le procès voir dossier* », « *violence avec arme par destination de M. X le patron* », « *reçu M. X remis dépôt plainte suite violence conjugale et éviction* », « *n'est pas de nationalité française* », « *alcoolique* »…

FICHE N°5

# L'UTILISATION DES CHAMPS LIBRES ET ZONES DE COMMENTAIRES

## RÉDIGER DES COMMENTAIRES OBJECTIFS ET JAMAIS EXCESSIFS OU INSULTANTS

La loi «Informatique et Libertés» (article 6) prévoit que les informations collectées doivent être adéquates, pertinentes et non excessives au regard de la finalité poursuivie. Ces règles sont valables à la fois pour les traitements automatisés et les traitements dits «papier». Les commentaires ne doivent donc pas être inappropriés, subjectifs ou insultants.

À titre illustratif, s'il peut paraître légitime qu'un bailleur social identifie dans un traitement automatisé un résident dont la situation particulière justifie un allégement ou un échelonnement de ses loyers, en revanche, renseigner le motif associé dans une zone de commentaire est souvent non pertinent voire excessif.

Il semble, en effet, qu'une telle information devrait plutôt figurer dans le dossier du locataire concerné et n'être accessible qu'aux seules personnes ayant un intérêt légitime à en connaître comme, par exemple, les employés chargés d'instruire les demandes de délais de paiement. Les employés uniquement chargés du recouvrement des loyers, sauf justification particulière, n'ont quant à eux pas besoin de connaître le motif associé au rééchelonnement des loyers.

De même, il peut être nécessaire de faire état du comportement d'un résident, notamment pour prévenir les personnes amenées à se rendre à son domicile. Pour autant, i**l ne faut renseigner que des mentions neutres et factuelles telles que**: «*échange difficile*», «*ne pas se rendre seul à son domicile*», **en lieu et place de précisions stigmatisantes** telles que «*résident complètement dingue*», «*résident alcoolique, drogué…*», «*résident violent*» ou «*résident pouvant facilement péter un plomb*».

## NE PAS RENSEIGNER D'INFORMATIONS SENSIBLES

Une attention particulière doit être accordée aux données dites «sensibles», c'est-à-dire celles visées par l'article 8-I de la loi «Informatique et Libertés» (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, données relatives à la santé ou à la vie sexuelle)

Par principe, la loi «Informatique et Libertés» interdit la collecte de telles données, que ce soit dans un traitement automatisé ou non. Les exceptions qui permettent de déroger à cette interdiction sont mentionnées à son article 8-II.

Parmi la liste de ces exceptions, seul le consentement exprès des personnes concernées semble de nature à justifier la collecte de telles données dans une zone de commentaires par un bailleur social. Le cas échéant, le responsable du traitement devrait dès lors être en mesure de justifier du recueil préalable de ce consentement, qui doit être libre et éclairé.

En raison des risques de dérives, et puisqu'une zone de commentaire est un outil accessoire dans la gestion administrative des dossiers des résidents, les hypothèses pouvant justifier une collecte de données sensibles dans une zone de commentaires sont rares, voire inexistantes.

**ATTENTION**

L'article 8-II-1° de la loi précise qu'un consentement exprès peut permettre la collecte de données sensibles, sauf dans les cas où la loi prévoit que l'interdiction ne peut être levée par le consentement de la personne concernée.

En effet, s'il s'agit de personnaliser une relation avec un résident, il est toujours possible de renseigner une information neutre et objective (*Cf. 2° ci-dessus*), par exemple en indiquant une attitude à adopter («*utiliser un vocabulaire simple*», «*parler fort et distinctement*», «*communiquer par écrit*»…) à la place de termes mettant en avant une affection ou un handicap («*débile léger*», «*sourd*», «*muet*»…) , comme la Commission a pu le constater à l'occasion de contrôles.

FICHE N°5

# L'UTILISATION DES CHAMPS LIBRES ET ZONES DE COMMENTAIRES

## RENDRE LES ZONES COMMENTAIRES ACCESSIBLES AUX SEULES PERSONNES LÉGITIMES À EN CONNAÎTRE

Lorsque des zones de commentaires sont utilisées, une politique d'habilitation permettant de limiter l'accès à leur contenu aux seules personnes ayant intérêt à en connaître dans le cadre de leurs attributions est obligatoire.

Par exemple, si ces zones ont vocation à personnaliser une relation avec des résidents, seules les personnes en contact régulier avec ces derniers doivent pouvoir y accéder. Il peut ainsi s'agir du gardien, à charge pour lui de communiquer les informations nécessaires aux autres personnes intervenant dans les logements.

## SENSIBILISER ET FORMER LES UTILISATEURS

De façon générale, une politique de sensibilisation à la protection de la vie privée des résidents est indispensable. Cette politique peut, par exemple, consister en des notes d'information ou des formations spécifiques.

La désignation d'un Correspondant informatique et libertés (CIL) est un relais efficace pour diffuser les bonnes pratiques, assurer des formations internes ou encore réaliser des audits réguliers.

En pratique, en ce qui concerne les zones de commentaires, la sensibilisation des utilisateurs peut également prendre la forme d'un message s'affichant automatiquement sur l'écran des utilisateurs au démarrage pour leur rappeler les règles à respecter.

*Exemple de message :*

*Attention, vous accéder à un espace vous permettant de renseigner librement des informations sur le compte des résidents.*

*Pour rappel, vous devez impérativement rédiger des commentaires objectifs et jamais excessifs ou insultants, à l'exclusion de toute donnée considérée comme sensible (origine raciale ou ethnique, opinions politiques, philosophiques ou religieuses, appartenance syndicale, données relatives à la santé ou à la vie sexuelle, infractions, condamnations, mesure de sûreté).*

*En cas de doute, vous pouvez contacter _____ . qui vous indiquera ce qu'il est possible de rédiger pour ne pas porter atteinte aux droits des résidents.*

*Pour information, sachez que cet espace fait régulièrement l'objet d'un nettoyage afin de supprimer toute donnée interdite et que les résidents peuvent accéder sur simple demande aux commentaires les concernant.*

FICHE N°5

# L'UTILISATION DES CHAMPS LIBRES ET ZONES DE COMMENTAIRES

## SURVEILLER ET NETTOYER RÉGULIÈREMENT LES ZONES COMMENTAIRES

En raison de la liberté de rédaction offerte aux utilisateurs, l'utilisation de zones de commentaires est susceptible de donner lieu à la diffusion de commentaires excessifs. Le responsable de traitement doit prendre en compte ce risque et prévoir des mesures pour le circonscrire.

Ces mesures peuvent par exemple consister à utiliser des listes de mots clefs interdits, entraînant la remontée d'une alerte à destination d'un modérateur ou ne pouvant tout simplement pas être enregistrés.

Un audit régulier des champs libres pour supprimer les commentaires excessifs apparaît également indispensable. Cette tâche pouvant être assurée par un employé ou automatisée grâce à un outil vérifiant les contenus des zones commentaires.

*Des extractions des commentaires peuvent être réalisées régulièrement pour s'assurer du respect de la loi « Informatique et Libertés ». Si ces extractions peuvent mener à des sanctions disciplinaires, une consultation des instances représentatives du personnel et une information individuelle des salariés est nécessaire.*

# FICHE N°6
# LE TRAITEMENT D'APPRÉCIATIONS SUR LES DIFFICULTÉS SOCIALES

*Les bailleurs sociaux peuvent être amenés à apprécier des difficultés sociales rencontrées par des résidents.*

*Au regard de la loi Informatique et Libertés, de telles appréciations sont considérées comme des données sensibles.*

*Dans quel cas et sous quelles conditions un bailleur social peut-il collecter de telles données ?*

## UN ACCOMPAGNEMENT DES PERSONNES VERS ET DANS LE LOGEMENT

De nombreux critères définis par le Code de la construction et de l'habitation sont pris en compte pour l'attribution de logements sociaux. Certains de ces critères sont déterminants pour désigner des personnes prioritaires (au titre de la loi DALO, par exemple).

Tel est le cas, par exemple, des personnes défavorisées, des personnes sans domicile ou logées dans des logements insalubres, des personnes et familles menacées d'expulsion sans relogement, les victimes de violences conjugales, les personnes handicapées, etc.

Au sein de chaque organisme bailleur, une commission est chargée d'attribuer nominativement les logements, notamment au regard de la situation sociale des demandeurs.

Dans le cadre de la gestion locative, des mesures d'aide individuelles sont parfois proposées aux personnes qui rencontreraient des difficultés, que ce soit pour l'installation ou pour le maintien dans le logement.

Certains bailleurs sociaux se sont en effet engagés dans l'accompagnement social de certaines personnes, par exemple en mettant en place des mesures pour les locataires en procédure d'expulsion, pour prévenir les risques d'impayés ou encore pour aider les personnes confrontées aux problèmes de précarité énergétique.

Il apparaît légitime qu'un bailleur social puisse apprécier des difficultés sociales dans ces hypothèses.

L'autorisation unique n°35 vise ainsi la collecte de telles appréciations dans le cadre de :

- l'instruction des demandes d'attribution, d'adaptabilité ou de mutation des logements, en particulier pour prendre en compte les décisions des Commissions d'attribution des logements ou des Commissions départementales de médiation;
- la mise en œuvre d'un suivi social personnalisé proposé aux personnes et familles en difficultés, lors de l'attribution d'un logement ou en cours de gestion locative, pour permettre une entrée et le maintien dans un logement ou favoriser une meilleure insertion.

FICHE N°6

# LE TRAITEMENT D'APPRÉCIATIONS SUR LES DIFFICULTÉS SOCIALES

## DES INFORMATIONS NÉCESSAIRES POUR DÉCIDER DE L'ATTRIBUTION D'UN LOGEMENT OU RÉALISER UN ACCOMPAGNEMENT SOCIAL

Un accompagnement individualisé et adapté proposé à une personne peut nécessiter de disposer d'informations qui la concerne, en particulier sur les difficultés qu'elle peut rencontrer.

Compte tenu de la sensibilité de ces données, susceptibles d'entraîner une forme de stigmatisation des personnes concernées, souvent vulnérables, leur traitement automatisé fait l'objet d'une attention particulière de la CNIL.

### PRÉCISION

Deux situations doivent être distinguées :

**a. une assistance sans suivi social :**

Lorsque l'aide apportée aux personnes consiste à les informer sur des démarches administratives à effectuer, par exemple auprès des gestionnaires d'aide au logement (CAF), à les aider à constituer un dossier ou à les mettre en relation avec les organismes compétents au regard de leur situation, le bailleur n'a pas à enregistrer ni à conserver les données relatives aux difficultés des personnes qu'il a eu à connaître lors de l'entretien avec l'intéressé.

En effet, seul l'organisme en charge de l'instruction de la demande peut collecter les données personnelles permettant le suivi des dossiers.

**b. un suivi social personnalisé des résidents :**

En cas de mise en place d'un suivi social effectif, les bailleurs peuvent être amenés à collecter et à enregistrer des informations relatives aux difficultés sociales des personnes pour l'attribution, la mutation ou l'adaptation d'un logement ainsi que dans le cadre d'un suivi social des locataires en situation précaire.

**Les informations collectées dans le cadre d'un suivi social doivent être pertinentes.**

Les informations demandées aux résidents ou futurs résidents doivent être strictement nécessaires à la compréhension de la situation de la personne concernée et à la recherche d'une solution adaptée.

L'accompagnement social répondant à des besoins individuels, la nature des informations collectées dépendra de la situation sociale de chaque personne et des demandes éventuellement formulées.

Par exemple, en cas d'impayés des loyers, il suffira dans certains cas d'analyser les ressources des personnes composant le foyer (salaires, allocations, prestations, etc.) pour appréhender les difficultés d'ordre économique et financier rencontrées.

Dans d'autres cas, une évaluation de la situation particulière du locataire sera nécessaire pour comprendre sa dette. Des éléments complémentaires (perte d'emploi, séparation, prise en charge d'un parent, existence d'un plan de surendettement etc.) pourront alors être demandés afin de trouver une solution permettant de résoudre les difficultés.

Souvent, l'accompagnement social implique qu'un bilan social de la situation du demandeur, reposant sur des éléments autres que socio-économiques, soit réalisé.

FICHE N°6

# LE TRAITEMENT D'APPRÉCIATIONS SUR LES DIFFICULTÉS SOCIALES

***La notion d'« appréciations » sur les difficultés sociales***

*Dès lors que les informations enregistrées dans un traitement automatisé résultent d'une évaluation d'une situation sociale à partir d'un faisceau d'informations (facteurs personnels et environnementaux), afin de déterminer l'aide à laquelle il est possible de prétendre ou pour permettre une prise de décision par le bailleur (aide financière, attribution du logement, apurement de la dette, abandon de la procédure d'expulsion, etc.),* **il s'agit alors d'un traitement comportant des appréciations sur les difficultés sociales.**

*En revanche, tel n'est pas le cas lorsqu'un bilan social de la situation du demandeur n'est pas réalisé et que le traitement se limite à l'enregistrement de données socio-économiques objectives (nature de la prestation demandée, ressources, nombre de personnes composant le foyer, aides au logement, bénéfices de prestations sociales, etc.).*

**ATTENTION**

Les informations qui n'ont pas d'incidence sur la compréhension des difficultés de la personne ou sur les aides qui pourraient lui être proposées ne doivent pas être enregistrées.

Par exemple, un bailleur ne peut recueillir des informations sur les conflits familiaux, même s'il en a connaissance, dès lors qu'ils ne justifient pas la situation du demandeur.

## UNE DURÉE DE CONSERVATION LIMITÉE ET ADAPTÉE À L'OBJECTIF POURSUIVI PAR LE TRAITEMENT

Les informations collectées pour l'attribution d'un logement ou dans le cadre d'un accompagnement social ne doivent pas être conservées indéfiniment.

La durée de conservation dépend en général du délai nécessaire à l'obtention d'un logement ou du temps nécessaire pour trouver des solutions aux besoins des personnes dans le cadre de leur accompagnement social.

Aussi, les données à caractère social doivent être supprimées dès lors que la décision d'attribution, d'adaptabilité ou de mutation d'un logement a été prise ou à la fin du suivi social.

Lorsque ce suivi est réalisé par un partenaire, le bailleur doit supprimer les informations dès qu'il a connaissance de la fin du suivi.

Avec l'accord de la personne concernée, afin de pouvoir s'appuyer sur l'historique des actions précédentes en cas de reprise ultérieure d'un suivi social, les données peuvent être conservées pendant cinq ans.

FICHE N°6

# LE TRAITEMENT D'APPRÉCIATIONS SUR LES DIFFICULTÉS SOCIALES

## DESTINATAIRES DES DONNÉES

L'instruction d'une demande de logement ou du suivi social personnalisé peut entraîner l'intervention ou le concours d'un ensemble de partenaires intervenant dans le secteur de l'action sociale (travailleurs sociaux, collectivités, associations spécialisées dans l'accompagnement social lié au logement, CAF, CCAS, etc.).

Par exemple, la commission d'attribution peut demander l'intervention d'un conseiller social afin qu'il réalise une enquête sociale qui déterminera s'il est nécessaire d'actionner certaines garanties avant l'attribution d'un logement (Locapass, FSL, accompagnement social…).

Certaines situations nécessitent de faire appel aux travailleurs sociaux des communes et à des associations spécialisées, notamment lorsque le bailleur ne dispose pas d'un service social. Par exemple, les centres communaux d'action sociale (CCAS) constituent un point d'entrée dans les dispositifs d'aides sociales légales (APL, FSL, etc.) et facultatives (aide financière ponctuelle octroyée par la commune).

Par ailleurs, les actions définies dans le cadre du plan départemental d'action pour le logement des personnes défavorisées (PDALPD), dont les objectifs sont notamment de permettre aux personnes ou familles en difficulté d'accéder à un logement décent et de disposer de la fourniture d'eau, d'énergie et du téléphone, sont mises en œuvre par un ensemble de partenaires (État, Conseil Général, CAF, communes, associations, bailleurs sociaux et privés, PACT et ADIL).

Aussi, les différentes mesures prises pour favoriser l'accès et le maintien dans le logement peuvent nécessiter une concertation entre différents acteurs et donner lieu à des échanges d'informations.

Les bailleurs peuvent donc être amenés à transmettre des informations recueillies auprès de la personne concernée et à l'inverse recevoir des informations leur permettant de prendre une décision.

### ATTENTION

**Les personnes faisant l'objet d'une appréciation sur les difficultés sociales qu'elles rencontrent doivent impérativement en avoir été préalablement informées.**

L'article 32 de la loi « Informatique et Libertés » impose, en effet, que le responsable du traitement informe les personnes concernées par ce dernier de son identité, de la finalité poursuivie, du caractère obligatoire ou facultatif des réponses, des conséquences d'un défaut de réponse, des destinataires ou catégories des destinataires des données, ainsi que des modalités d'exercice des droits des personnes (droit d'accès, de rectification et d'opposition pour motif légitime).

En tout état de cause, chaque intervenant ne doit accéder qu'aux données strictement nécessaires à l'accomplissement de sa mission. Par exemple, lorsqu'une évaluation sociale est effectuée à la demande de la commission d'attribution, seul le conseiller doit avoir accès à l'évaluation sociale intégrale. La commission ne doit être destinataire que des données administratives et des informations sur le type de démarches entreprises, l'ouverture d'un droit, ou encore la décision préconisée par le conseiller.

Les informations relatives aux difficultés rencontrées au stade de la demande de logement n'ont pas vocation à figurer dans le dossier de gestion locative, sauf exceptions dûment justifiées. À titre illustratif, les éventuelles données relatives aux conflits familiaux ne sont pas censées figurer dans le dossier de gestion locative.

Enfin, l'accès aux données doit être défini en fonction du besoin réel de chaque employé pour mener telle ou telle opération (création de profil, lecture, écriture, modification, suppression de profil dans le traitement).

# FICHE N°7
# LE TRAITEMENT DE DONNÉES RELATIVES À LA SANTÉ

*Pour l'exercice de leurs missions, sous certaines conditions, les bailleurs sociaux peuvent avoir besoin de collecter et traiter des données relatives à la santé des candidats ou des résidents. Dans quels cas ? Sous quelles conditions ?*

## QU'ENTEND-ON PAR « DONNÉES RELATIVES À LA SANTÉ » ?

Toute information permettant d'identifier la nature d'une affection, d'un handicap ou d'une déficience (catégorie ou codification) doit être considérée comme une donnée de santé.

En revanche, quand le degré de généralité d'une mention (« hôpital », « établissement spécialisé », « présence d'un handicap (oui/non) ») ne révèle pas la pathologie de la personne concernée, et ne porte pas atteinte à sa vie privée, il ne s'agit pas d'une donnée de santé.

Lorsqu'il intervient dans le cadre de ses missions, un bailleur social doit privilégier la collecte et le traitement (en veillant à ce que cela soit justifié) de données « génériques » aux lieux et places de données de santé. Par exemple, plutôt que de mentionner la « surdité » d'un résident, il peut être précisé qu'il convient d'échanger avec cette personne par écrit ou en langues des signes. De même, plutôt que de préciser qu'un résident est suivi pour troubles psychiatriques, il est par exemple préférable d'enregistrer la mention « ne pas se présenter seul au domicile ».

*En résumé : Privilégier des données commandant une action à la place de données mettant en lumière une affection, un handicap ou une déficience.*

## SEULES LES DONNÉES STRICTEMENT NÉCESSAIRES À L'EXERCICE DES MISSIONS DU BAILLEUR SOCIAL DOIVENT ÊTRE COLLECTÉES ET TRAITÉES

Le caractère sensible des données relatives à la santé impose d'encadrer strictement les traitements dans lesquels elles sont enregistrées.

Si un bailleur social peut avoir besoin de disposer de données relatives à la santé des résidents, pour l'exercice de certaines de missions particulières, en revanche, il ne peut en collecter et en disposer sans limite.

Une telle collecte doit nécessairement être indispensable au regard des missions d'un bailleur social et proportionnée par rapport à la finalité poursuivie, ce qui revient à dire qu'il ne doit pas être possible d'atteindre le but recherché sans avoir besoin de collecter des données de santé.

À titre illustratif, les bailleurs sociaux peuvent collecter des données de santé pour répondre aux demandes d'attribution de logements, aux demandes de mutation géographique ou encore d'adaptation d'un logement. Mais dans toutes ces hypothèses, ils doivent justifier du caractère pertinent et proportionné de la collecte.

FICHE N°7

# LE TRAITEMENT DE DONNÉES RELATIVES À LA SANTÉ

*En résumé : Avant de collecter des données relatives à la santé, un bailleur social doit se demander si cela est justifié au regard de ses missions et indispensable par rapport à ce qu'il envisage d'en faire.*

## L'INFORMATION DES PERSONNES ET LES AUTRES CONDITIONS DE COLLECTE ET DE TRAITEMENT DES DONNÉES RELATIVES À LA SANTÉ

Le fait qu'un un résident transmette des données de santé le concernant à son bailleur ne suffit pas, en soi, à autoriser le traitement de ces données. D'autres conditions sont en effet requises :

- la finalité poursuivie doit être déterminée et légitime (gestion et suivi des attributions ou demandes de mutations, accompagnement social de personnes en difficultés, ...) ;
- les données doivent être collectées de manière loyale et licite (par exemple, les informations doivent provenir directement du résident, et non de son entourage, si le résident est juridiquement capable), ce qui implique notamment d'en informer les personnes concernées et de recueillir leur consentement au préalable ;
- les données doivent être pertinentes et non excessives (par exemple, il n'est pas pertinent de collecter des informations relatives au statut virologique d'un résident pour instruire sa demande d'équipement spécialisé) ;
- les données ne doivent pas être conservées au-delà de la durée nécessaire à la finalité poursuivie ;
- seules les personnes habilitées doivent pouvoir y accéder, et ce, exclusivement pour l'exercice de leurs missions ;
- des mesures techniques et organisationnelles doivent garantir la sécurité et la confidentialité des données.

Dès lors que ces conditions sont réunies, le consentement exprès (c'est-à-dire explicite et non équivoque, ce qui suppose une information préalable) des résidents concernés permet de collecter et de traiter des données relatives à la santé. Dans cette hypothèse, le fichier doit être déclaré à la CNIL (déclaration normale ou engagement de conformité à la norme simplifiée n° 20 si les conditions de cette dernière sont réunies).

**PRÉCISION**

Il est toujours préférable de recueillir un consentement exprès par écrit, ne serait ce que pour être en mesure de justifier qu'il a été effectivement donné.

S'agissant de la situation des personnes vulnérables, le bailleur doit se rapprocher du représentant légal du résident afin de recueillir le consentement exprès de ce dernier. Si un tel représentant n'a pas été désigné, seul le résident peut valablement autoriser et initier la collecte de données relatives à sa santé.

**PRÉCISION**

Pour qu'un résident puisse valablement consentir, il doit préalablement être pleinement informé sur les raisons et les conditions de la collecte envisagée (cf. fiche sur l'information des personnes) conformément aux dispositions de l'article 32 de la loi « Informatique et Libertés ».

FICHE N°7

# LE TRAITEMENT DE DONNÉES RELATIVES À LA SANTÉ

*En résumé : Le consentement d'un résident nécessite au préalable une information claire, complète et intelligible. En outre, ne peuvent être traitées que les données strictement nécessaires par rapport à l'objectif poursuivi, qui doit évidemment être légitime, et ce, dans des conditions de nature à garantir la confidentialité des données.*

## LA CONSERVATION DES DONNÉES DE SANTÉ PAR UN PRESTATAIRE EXTÉRIEUR : L'AGRÉMENT HÉBERGEUR

Le dispositif légal relatif à l'agrément « hébergeur de données de santé » encadre la conservation et la restitution des données de santé par un tiers prestataire.

*L'article L. 1111-8 du code de la santé publique prévoit en effet que « les professionnels de santé ou les établissements de santé ou la personne concernée peuvent déposer des données de santé à caractère personnel, recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins, auprès de personnes physiques ou morales agréées à cet effet ».*

*En résumé : Si des données relatives à la santé sont hébergées par un prestataire, ce dernier doit être agréé à cet effet. La liste des hébergeurs de données de santé agréés est disponible sur le site internet de l'ASIP Santé (http://esante.gouv.fr/services/referentiels/securite/hebergeurs-agrees).*

## SENSIBILISER ET FORMER LES UTILISATEURS

De façon générale, une politique de sensibilisation à la protection de la vie privée des résidents est indispensable. Un telle politique apparaît d'autant plus nécessaire dès lors que des données sensibles sont collectées, au nombre desquelles figurent en particulier les données relatives à la santé.

Cette politique peut, par exemple, consister en des notes d'information ou des formations spécifiques.

La désignation d'un Correspondant informatique et libertés (CIL) est également un relais efficace pour diffuser les bonnes pratiques, assurer des formations internes ou réaliser des audits réguliers.

# FICHE N°8
# LES DONNÉES RELATIVES À DES INFRACTIONS, CONDAMNATIONS OU MESURES DE SÛRETÉ

*Les infractions, les condamnations et les mesures de sûreté sont des données sensibles, dont le traitement doit être encadré et réservé à certains organismes.*

*Dans quel cas et sous quelles conditions un bailleur social peut-il en collecter ?*

## QUI PEUT COLLECTER CE TYPE DE DONNÉES

La loi « Informatique et Libertés » (article 9) limite la possibilité de créer un fichier relatif à des infractions, condamnations ou mesures de sûreté aux :

- juridictions, autorités publiques, et personnes morales gérant un service public dans le cadre de leurs attributions ;
- auxiliaires de justice pour exercer les missions que la loi leur confie ;
- personnes physiques ou morales victimes pour exercer une action en justice ;
- sociétés de perception et de répartition des droits d'auteur et organismes de défense du droit d'auteur.

### FOCUS

***Les victimes***

L'article 9-3° de la loi « Informatique et Libertés » prévoyait que les victimes pouvaient collecter des données d'infractions. Cet article a été censuré par le Conseil constitutionnel, pour des motifs liés à une rédaction trop imprécise.

Toutefois, par une réserve d'interprétation, le Conseil a précisé que cette censure ne devait pas avoir pour effet de priver les personnes physiques et morales victimes de la possibilité de collecter des données relatives à des infractions, et ce, pour faire valoir un droit en justice.

C'est pourquoi les victimes, alors qu'elles ne figurent pas formellement dans la liste limitative des organismes pouvant créer un ficher d'infractions, peuvent néanmoins collecter des données d'infractions relatives à leurs contentieux.

Au-delà de ces hypothèses, c'est-à-dire pour les organismes qui ne sont pas visés par l'article 9 de la loi « Informatique et Libertés », une disposition législative doit permettre le traitement de données relatives à des infractions ou mesure de sureté. À défaut, une telle collecte est impossible.

FICHE N°8

# LES DONNÉES RELATIVES À DES INFRACTIONS, CONDAMNATIONS OU MESURES DE SÛRETÉ

## LES BAILLEURS SOCIAUX ET LE TRAITEMENT DE DONNÉES D'INFRACTION

Dans le cadre d'une activité normale, les bailleurs sociaux peuvent être amenés à collecter des données relatives à des infractions, condamnations ou mesures de sûreté.

Ils doivent, en effet, garantir la jouissance paisible des logements, ce qui les conduit à assurer la tranquillité et la sécurité des résidents et de leurs personnels.

Les bailleurs sont également fondés à traiter des données d'infractions pour lutter contre les actes d'incivilité ou de vandalisme contre leur patrimoine.

La loi « Informatique et Libertés » (article 25-I-3°) prévoit que les traitements relatifs aux infractions, condamnations ou mesures de sûreté doivent être autorisés par la CNIL.

La CNIL peut autoriser par une décision unique, appelée « autorisation unique », une catégorie de traitements correspondant aux mêmes finalités, portant sur des catégories de données identiques et ayant les mêmes destinataires ou catégories de destinataires.

Le pack de conformité dédié aux acteurs du logement social a été l'occasion pour la CNIL d'adopter une autorisation unique ouvrant aux bailleurs sociaux la possibilité, sous certaines conditions, de collecter des données relatives aux infractions, condamnations ou mesure de sûreté (autorisation unique n° 34).

Cette autorisation unique concerne plus précisément la gestion de précontentieux et de contentieux, notamment en matière :

- de trouble anormal de voisinage ;
- de recouvrement des impayés ;
- d'expulsion locative ;
- d'atteintes au patrimoine immobilier ou aux personnes.

Cette autorisation unique comporte également une sous finalité qui permet aux bailleurs sociaux de mettre concrètement en application certaines décisions de justice, lorsqu'elles ont une incidence sur un lieu de résidence (ex : jugement d'éloignement d'un résident violent).

Il semble en effet pertinent qu'un bailleur puisse avoir connaissance de cette information, à l'initiative de la personne concernée, notamment pour ne pas reloger la personne éloignée trop près.

En dehors de ces cas, les bailleurs n'ont en principe pas vocation à traiter des données relatives à des infractions.

Toutefois, des textes spécifiques peuvent, dans certaines hypothèses particulières, fonder les bailleurs à traiter des données relatives à des infractions, notamment en matière de prévention de la délinquance.

### ATTENTION

La raison à l'origine de la condamnation ne doit pas être renseignée dans le système d'information d'un bailleur social, puisque cette information ne présente pas d'intérêt dans le cadre d'un relogement.

## LES DESTINATAIRES

Ne peuvent accéder à des données relatives à des infractions, condamnations ou mesure de sûreté que :

- les employés habilités dans le cadre de leurs fonctions à gérer et suivre les litiges amiables et les procédures contentieuses, ainsi qu'à mettre en application les décisions de justice ayant une incidence sur un lieu de résidence;
- les auxiliaires de justice et officiers ministériels ;
- l'autorité judiciaire saisie d'un litige ;
- les organismes tiers autorisés par une disposition légale à obtenir la communication de données à caractère personnel relatives à des précontentieux, contentieux ou condamnations.

FICHE N°8

# LES DONNÉES RELATIVES À DES INFRACTIONS, CONDAMNATIONS OU MESURES DE SÛRETÉ

## PRÉCISIONS

En raison de la sensibilité des données relatives aux infractions, condamnations et mesure de sûreté, il est impératif que le système d'information comporte une fonctionnalité de traçabilité des accès à l'application, d'une part, ainsi que des opérations effectuées sur ces données, d'autre part (Cf. fiche sécurité).

## CAS PARTICULIERS

### Le gardiennage et la surveillance des immeubles

En application de l'article L. 271-1 du code de la sécurité intérieure, certains bailleurs sociaux peuvent être obligés d'assurer le gardiennage ou la surveillance des locaux dont ils sont responsables.

Pour cela, il faut que l'importance des immeubles ou leur situation le justifie, d'une part, et qu'un décret en Conseil d'Etat prévoit que cette obligation s'impose dans la zone géographique concernée, d'autre part.

Si l'exercice de cette mission particulière donne lieu à la collecte de données d'infractions, dans un traitement automatisé ou non, deux situations sont envisageables :

- s'il s'agit de données en rapport avec une atteinte au personnel du bailleur ou à son patrimoine (agression, tag, dégradation…) qui sont utilisées dans le cadre d'un précontentieux ou d'un contentieux avec l'auteur présumé, ces données peuvent être traitées sur la base de l'autorisation unique n° 34 ;
- dans les autres cas, le responsable du traitement devra obtenir une autorisation spécifique de la CNIL (demande d'autorisation), en justifiant notamment à cette occasion de la pertinence et de la proportionnalité du traitement.

### La transmission des images d'un dispositif vidéo aux forces de l'ordre

Lors de circonstances faisant redouter la commission d'atteintes aux biens ou aux personnes, un bailleur social peut transmettre, de manière occasionnelle ou en temps réel, les images enregistrées aux services de police et de gendarmerie (article L. 126-1-1 du code de la construction et de l'habitation).

Ce type de transmission doit être autorisé par une décision de la majorité des copropriétaires ou, dans les ensembles immobiliers à caractère social, par une décision du gestionnaire.

Par ailleurs, une convention doit être conclue entre le Préfet et le gestionnaire de l'immeuble et, lorsqu'il est prévu de transmettre des images aux services de police municipale, elle doit en outre être signée par le maire. La convention doit préciser les conditions et les modalités du transfert des images et être transmise à la Commission départementale de vidéoprotection, pour qu'elle apprécie les garanties et puisse demander leur renforcement au Préfet.

La transmission des images doit être limitée au temps nécessaire à l'intervention des services de l'ordre. L'existence de ce système de vidéosurveillance et la possibilité de transmission des images aux forces de l'ordre doivent être affichées sur place.

Les images transmises aux forces de l'ordre ne peuvent porter sur l'entrée des habitations privées ou sur la voie publique.

*Si un bailleur souhaite pouvoir transmettre des images en temps réel aux forces de l'ordre, il doit d'abord effectuer une déclaration normale auprès de la CNIL.*

*À cette occasion, il convient de transmettre à la CNIL une copie de la convention conclue en application du code de la construction et de l'habitation, ainsi que de l'avis Commission départementale de vidéoprotection.*

FICHE N°8

# LES DONNÉES RELATIVES À DES INFRACTIONS, CONDAMNATIONS OU MESURES DE SÛRETÉ

**En dehors de ces hypothèses, les forces de police ne sont pas censées accéder aux enregistrements vidéo d'un bailleur, sauf à justifier d'une réquisition judiciaire.**

## Les conseils locaux de sécurité (CLSPD) et les zones de sécurité prioritaires (ZSP)

Dans le cadre des politiques publiques de prévention de la délinquance menées par la municipalité dans les CLSPD ou sous la responsabilité des forces régaliennes de l'Etat, notamment dans les ZSP, des demandes de transmission d'information sur certaines personnes peuvent être effectuées par les autorités publiques.

Il ne s'agit pas uniquement d'informations d'« ambiance » permettant aux forces de l'ordre de s'informer sur l'atmosphère d'une zone de vie commune, mais d'obtenir des informations précises sur certains individus ciblés.

Ces échanges d'information portant sur des personnes identifiées peuvent être réalisés de manière orale et ponctuelle, mais parfois ils peuvent être institutionnalisés, c'est-à-dire prendre des formes récurrentes et même écrites, entre les bailleurs et les forces de police municipale ou nationale. Elles peuvent concerner différentes informations telles que des appréciations sociales sur les personnes, le relevé d'activités supposées illicites, la constatation d'incivilités, etc.

Or, ces échanges d'information sans le consentement des personnes concernées sont très intrusifs dans leur vie privée et peuvent poser problème quant à l'exercice de leurs libertés individuelles. Par conséquent, ces transferts de données ne sont pas pris en compte dans le pack de conformité.

Toutefois, si le bailleur social était contraint de participer à ces échanges d'information sur des personnes identifiées, il devra se conformer aux dispositions de la loi « Informatique et Libertés ».

Des conventions peuvent être mises en place entre le bailleur et les services de gendarmerie ou de polices. Il est impératif que la CNIL soit associée à ces conventions, dès lors que des échanges portent sur des données à caractère personnel relatives à des appréciations sur des difficultés sociales ou à des infractions, des condamnations ou des mesures de sûreté.

Tout traitement de données mis en œuvre dans ce cadre doit faire l'objet d'une demande d'autorisation auprès de la CNIL.

La CNIL prépare actuellement, en collaboration avec les acteurs publics concernés, un encadrement réglementaire adapté à ce genre d'échanges permettant de concilier l'intérêt général de la prévention de la délinquance avec les limitations et précautions indispensables permettant de concilier cette politique publique avec la protection de la vie privée et des libertés individuelles.

# FICHE N°9
# L'INFORMATION DES PERSONNES

*La loi « Informatique et Libertés » prévoit que les personnes auprès desquelles des données à caractère personnel sont collectées doivent bénéficier d'une information avant la collecte. Sur quoi doit porter cette information ? Comment la délivrer ?*

## L'OBLIGATION D'INFORMER LES PERSONNES

L'article 32 de la loi « Informatique et Libertés » impose que les personnes concernées par un traitement de données à caractère personnel soit informées :

- de l'identité du responsable de traitement,
- de la finalité poursuivie,
- du caractère obligatoire ou facultatif des réponses,
- des conséquences éventuelles d'un défaut de réponse,
- des destinataires ou catégories de destinataires,
- de l'existence et des modalités d'exercice des droits d'accès, de rectification et d'opposition pour motif légitime,
- le cas échéant, des transferts de données réalisées à destination de pays situés en dehors de l'Union européenne.

**PRÉCISIONS**

Lorsque des formulaires sont utilisés pour collecter les données, ces derniers doivent impérativement porter mention des éléments visés au 1er, 2ème, 3ème et 6ème tirets.

S'il n'est pas obligatoire de faire en sorte que l'information délivrée porte sur le détail des données collectées, le responsable de traitement doit néanmoins communiquer cette information aux personnes qui en font la demande.

## EXEMPLES DE MENTIONS INFORMATIVES

**Mention d'information à porter sur les formulaires de collecte**

*Le(s) service(s) _____ (citer le nom du ou des services responsables du traitement) dispose(nt) de moyens informatiques destinés à gérer plus facilement _____ _____ (indiquer la finalité du traitement).*

*Conformément à la loi « Informatique et Libertés » du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant à _____ (préciser le service et l'adresse).*

*Vous pouvez également, pour des motifs légitimes, vous opposer au traitement des données vous concernant.*

FICHE N°9

# L'INFORMATION DES PERSONNES

## Mention d'information à porter sur les formulaires de collecte

*Le(s) service(s) _____ (citer le nom du ou des services responsables du traitement) dispose(nt) de moyens informatiques destinés à gérer plus facilement _____ (indiquer la finalité du traitement).*

*Les informations enregistrées sont réservées à l'usage du (ou des) service(s) concerné(s) et ne peuvent être communiquées qu'aux destinataires suivants : _____ (préciser les destinataires).*

*Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, toute personne peut obtenir communication et, le cas échéant, rectification ou suppression des informations la concernant, en s'adressant au service _____ _____(citer le nom du service ou des services concernés).*

## Panneau d'information en matière de vidéoprotection

Ce panneau doit être situé a l'entrée de l'établissement et visible par les salariés et les personnes extérieures.


## Mention d'information à porter sur les formulaires de collecte

*Un dispositif destiné au contrôle de l'accès _____ (préciser ici la zone concernée) a été mis en place par _____ (identification du responsable du traitement) pour _____ (préciser ici la finalité).*

*Seules les personnes habilitées du service _____ (préciser le service – par exemple le service informatique) auront accès à vos données.*

*Conformément à la loi « Informatique et Libertés » du 6 janvier 1978 modifiée, vous pouvez avoir accès et rectifier les informations qui vous concernent en vous en adressant à _____ (préciser le service et l'adresse du service chargé de répondre aux demandes de droit d'accès).*

# FICHE N°10
# SÉCURITÉ DES DONNÉES

*L'article 34 de la loi « Informatique et Libertés » impose à un responsable de traitement de prendre toutes les précautions utiles pour préserver la sécurité des données dont il est responsable, en fonction de leur nature et des risques supposés. Il doit en particulier empêcher l'accès à ces données aux tiers non autorisés à les consulter.*

*Un bailleur social doit ainsi prendre un certain nombre de précautions lorsqu'il envisage de conserver, de communiquer ou de rendre accessibles des données à caractère personnel.*

*La sécurisation d'un système d'information exige de prendre en compte tous les aspects de sa gestion, tant au niveau organisationnel que technique, ainsi que réévaluer régulièrement les mesures initialement prises.*

## L'AUTHENTIFICATION DES UTILISATEURS

Le responsable d'un système informatique doit s'assurer que chaque utilisateur ne peut accéder qu'aux seules données dont il a besoin pour l'exercice de son activité.

Pour cela, chaque utilisateur doit disposer d'un identifiant unique et s'authentifier avant d'accéder au système.

Les mécanismes permettant d'authentifier les utilisateurs peuvent, par exemple, prendre la forme de mots de passe rattachés à un identifiant ou à une carte à puce.

Les identifiants des utilisateurs doivent être différents des comptes définis par défaut par les éditeurs de logiciels.

Lorsque l'authentification ou l'identification des utilisateurs est assurée par de mots de passe, la CNIL considère que ceux-ci doivent être constitués d'au moins huit caractères, à choisir parmi trois types différents (majuscules, minuscules, chiffres, caractères spéciaux), et être régulièrement renouvelés, par exemple tous les six mois.

### PRÉCISIONS

Les mots de passe des comptes définis par défaut par les éditeurs doivent être modifiés par les utilisateurs, dès leur première connexion.

Aucun compte usager ne doit être partagé entre plusieurs utilisateurs.

## LA GESTION DES HABILITATIONS

Chaque utilisateur ne devant accéder qu'aux données strictement nécessaires à l'exercice de son activité professionnelle, des profils d'habilitation doivent être définis pour déterminer les types de données accessibles à une catégorie d'utilisateur.

Une procédure de gestion des habilitations doit être formalisée afin d'assurer leur mise à jour, notamment pour supprimer les permissions d'accès des utilisateurs qui ne sont plus habilités ou qui ont quitté l'organisme.

FICHE N°10
# SÉCURITÉ DES DONNÉES

Cette procédure doit également prévoir des contrôles des habilitations afin de s'assurer que les permissions d'accès aux données ne sont pas détournées (par exemple, partage d'un seul compte utilisateur utilisé par différentes personnes).

## SENSIBILISATION DES UTILISATEURS ET FORMALISATION DES RÈGLES DE SÉCURITÉ

Une charte informatique, qui doit être annexée au règlement intérieur, peut être rédigée afin d'informer et responsabiliser les usagers, notamment sur les points suivants :

- **Le rappel des règles de protection des données** et les sanctions encourues en cas de non respect de la loi.
- **Le champ d'application de la charte**, qui inclut notamment :
  - les modalités d'intervention du service de l'informatique interne, notamment en cas de télémaintenance ;
  - les moyens d'authentification ;
  - les règles de sécurité auxquelles se conformer, ce qui peut inclure par exemple de :
  - signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
  - ne jamais confier son moyen d'authentification à un tiers (identifiant/mot de passe, carte à puce et code PIN, etc.) ;
  - ne pas modifier les paramétrages du poste de travail ;
  - ne pas installer, copier, modifier, détruire des logiciels sans autorisation ;
  - verrouiller son ordinateur dès que l'on quitte son poste de travail ;
  - ne pas accéder, tenter d'accéder, ou supprimer des informations qui ne relèvent pas des tâches incombant à l'utilisateur ;
  - définir les modalités de copie de données sur un support externe ;
  - sensibiliser sur les risques d'hameçonnage (« *phishing* ») et autres méthodes d'acquisition déloyale d'information ;
  - sécuriser les outils personnels utilisés dans un cadre professionnel (BYOD).
- **Les modalités d'utilisation des moyens informatiques et de télécommunications** mis à disposition comme :
  - le poste de travail ;
  - les équipements nomades ;
  - l'espace de stockage individuel ;
  - le réseau local ;
  - Internet ;
  - la messagerie électronique ;
  - le téléphone.
- **Les conditions d'administration du système d'information**, et l'existence, le cas échéant, de :
  - systèmes automatiques de filtrage des accès aux matériels et aux applications ;
  - systèmes automatiques de traçabilité ;
  - gestion du poste de travail.
- **Les responsabilités et sanctions encourues en cas de non respect de la charte.**

## LA SÉCURITÉ DES POSTES DE TRAVAIL

La sécurité des postes de travail implique notamment des mesures permettant de prévenir les tentatives d'accès frauduleux, l'exécution d'un virus ou la prise de contrôle à distance, notamment par Internet.

Il est ainsi conseillé de limiter le nombre de tentatives infructueuses d'accès à un compte utilisateur. En fonction du contexte (nature des données, nombre de dossiers accessibles, etc.), le nombre de tentatives

FICHE N°10
# SÉCURITÉ DES DONNÉES

autorisées par le système peut varier de cinq à dix. Lorsque la limite est atteinte, le compte en question doit être bloqué, temporairement ou jusqu'à l'intervention d'un administrateur du système.

Il est également conseillé d'installer un pare-feu logiciel (firewall), pour contrôler les communications entrantes et sortantes, ainsi que de limiter les ports logiciels de communication à ceux qui sont strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail (par exemple le port 80 pour l'accès http à Internet, le port 443 pour l'accès https, etc.).

Les antivirus ainsi que tous les autres logiciels utilisés doivent être régulièrement mis à jour.

Un verrouillage automatique des sessions à l'issue d'une période d'inactivité permet d'améliorer la sécurité globale du système. S'agissant de l'accès à une application métier, la fermeture d'une session après cinq minutes d'inactivité permet d'améliorer la sécurité sans entraîner de gène excessive dans l'activité de l'utilisateur.

## LES MESURES DE SAUVEGARDES ET L'ARCHIVAGE

Des copies de sauvegarde des données à caractère personnel peuvent être effectuées, conformément à une politique de sauvegarde.

Une sécurisation renforcée est requise pour les sauvegardes des données sensibles ou jugées confidentielles par l'organisme (par exemple par une mesure de chiffrement ou une traçabilité renforcée des accès et des opérations effectuées sur les sauvegardes).

Concernant les possibilités de conservation des données, on distingue habituellement trois catégories de stockage :

- **Les bases actives :** les données d'utilisation courante par les services en charge de la mise en œuvre du traitement,
- **Les archives intermédiaires :** les données qui ne sont plus utilisées mais présentant encore un intérêt administratif pour l'organisme (par exemple le temps d'une prescription). Ces données sont conservées de manière distincte et leur consultation doit être ponctuelle et motivée, par des personnes spécifiquement habilitées.
- **Les archives définitives :** les données présentant un intérêt historique ou statistique justifiant qu'elles ne fassent l'objet d'aucune destruction (par exemple, le cas d'archives pour le compte de l'État). Ces archives doivent également faire l'objet de mesures spécifiques visant à assurer leur intégrité.

Par ailleurs, une sauvegarde des logiciels servant au traitement peut être également prévue afin de garantir la pérennité de ce dernier.

**RAPPEL**

Les archives doivent être sécurisées et chiffrées si les données archivées sont des données sensibles ou jugées confidentielles par l'organisme.

## LA MAINTENANCE

Lors de la maintenance et des interventions techniques, la sécurité des données doit être garantie. La confidentialité des données peut être garantie en prévoyant par exemple d'enregistrer les interventions de maintenance dans une main courante et d'encadrer les interventions effectuées par un responsable de l'organisme.

En cas d'assistance sur les postes de travail, les outils d'administration à distance doivent être configurés de manière à recueillir l'accord de l'utilisateur avant toute interven-

FICHE N°10
# SÉCURITÉ DES DONNÉES

tion sur son poste, par exemple en cliquant sur une icône ou en répondant à un message s'affichant à l'écran. L'utilisateur doit également pouvoir constater si la prise en main à distance est en cours et quand elle se termine, par exemple grâce à l'affichage d'un message à l'écran.

Les données présentes sur les matériels destinés à être mis au rebut doivent être supprimées par une procédure d'effacement sécurisé ou par une destruction physique du matériel. Par conséquent, une inspection du matériel doit être effectuée pour s'assurer que toute donnée a bien été supprimée de façon sécurisée.

## LA TRAÇABILITÉ

Afin d'être en mesure d'identifier a posteriori un accès frauduleux à des données personnelles, une utilisation abusive de telles données ou de déterminer l'origine d'un incident, il convient d'enregistrer les actions effectuées sur le système informatique.

Le système doit ainsi enregistrer les événements (accès à l'application, accès et opérations sur les données), garantir que ces enregistrements ne peuvent être altérés et conserver ces éléments pendant une durée non excessive. Ces événements sont composés de traces fonctionnelles (traces relatives au fonctionnement de l'application métier), de traces techniques (traces relatives au fonctionnement des éléments réseau et système mis en œuvre sur le système d'information) et de traces embarquées (traces inscrites dans des documents, par exemple, pour en certifier l'origine).

À cet effet, il peut être nécessaire de prévoir un système de journalisation (c'est-à-dire un enregistrement dans des « fichiers de logs ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité. Ces journaux doivent conserver les événements sur une période glissante ne pouvant excéder six mois (sauf obligation légale ou autorisation par la CNIL).

Il faudra dans ce cas prévoir au minimum la journalisation des accès des utilisateurs incluant leur identifiant, la date et l'heure de leur connexion, ainsi que la date et l'heure de leur déconnexion. En cas d'opérations effectuées sur les données sensibles, il est nécessaire de conserver également le détail des actions effectuées par l'utilisateur, telles que par exemple les données consultées ou modifiées. Par ailleurs, les données de journalisation ne doivent être utilisées que pour leur finalité annoncée d'identification a posteriori en excluant toute autre finalité comme par exemple le contrôle des horaires ou la vérification du travail effectué. Dans tous les cas, ces traces devront être régulièrement analysées afin de détecter tout comportement suspect ou anormal.

## L'ÉCHANGE D'INFORMATION AVEC D'AUTRES ORGANISMES

La communication de données à caractère personnel doit être sécurisée. La messagerie électronique et le fax, même s'ils apportent un gain de temps, ne constituent pas a priori un moyen de communication sûr pour transmettre des données personnelles. Une simple erreur de manipulation peut conduire à la divulgation d'informations personnelles à des destinataires non habilités et à porter ainsi atteinte au droit à la vie privée des personnes. En outre, la transmission via Internet de données nominatives comporte, compte tenu de l'absence générale de confidentialité du

FICHE N°10
# SÉCURITÉ DES DONNÉES

réseau Internet, des risques importants de divulgation de ces données et d'intrusion dans les systèmes informatiques internes par exploitation de ces données frauduleusement acquises.

Dans tous les cas, la transmission du secret (clé de déchiffrement, mot de passe, etc.) garantissant la confidentialité du transfert doit s'effectuer de manière distincte, si possible via un canal de nature différente (par exemple, envoi d'un fichier chiffré par courriel et communication du mot de passe par SMS).

Concernant la confidentialité d'une communication, il est possible de chiffrer directement les données ou le canal de transmission lors d'un envoi via un réseau. En cas de transfert matériel (copie sur DVD ou clé USB par exemple), les données peuvent être chiffrées préalablement à leur enregistrement sur le support physique. Si une transmission utilise la messagerie électronique, le chiffrement des pièces à transmettre est alors indispensable. Si les document transmis par voie électronique n'est pas chiffré, il sera alors indispensable de chiffrer le canal de transmission. A cet effet, l'utilisation du protocole SSL/TLS garantit l'authentification des serveurs (ainsi qu'éventuellement celle des clients) et la confidentialité des communications (SFTP pour le transfert de fichiers ou HTTPS pour les services Web sont des protocoles de transmission sécurisée).

**PRÉCISION**

Un portail sécurisé, sous la forme d'un service Web associé à l'utilisation du protocole SSL, garantit la confidentialité des échanges de données entre divers organismes. Un tel portail associé à l'identification des usagers permet également de limiter l'accès aux données aux seules personnes habilitées.

## L'ANONYMISATION

Le terme d'anonymisation est réservé aux opérations irréversibles. On utilise le terme de pseudonymisation lorsque l'opération est réversible.

Une anonymisation irréversible consiste à supprimer tout caractère identifiant à un ensemble de données. Concrètement, cela signifie que toutes les informations directement ou indirectement identifiantes sont supprimées ou modifiées, rendant impossible toute ré-identification des personnes.

La pseudonymisation est une technique qui consiste à remplacer un identifiant (ou plus généralement des données à caractère personnel) par un pseudonyme. Cette technique permet la ré-identification ou l'étude de corrélations en cas de besoin particulier.

Lors d'une pseudonymisation, il faut être vigilant dans la mesure où une ré-identification peut intervenir à partir d'informations partielles (par exemple, la combinaison des données ville et date de naissance peut être suffisante).

*Exemple de pseudonymisation :*
*Une pseudonymisation limitant efficacement le risque de ré-identification directe peut par exemple être effectuée en générant une clé secrète longue et difficile à mémoriser (une combinaison de caractères aléatoires), puis en appliquant une fonction dite à sens unique sur les données (par exemple, un algorithme de hachage à clé secrète tel HMAC). En l'absence de besoin de ré-identification efficace, la clé secrète peut être supprimée pour diminuer le risque de ré-identification. Si la conservation de la clé secrète est nécessaire, des mesures doivent être mises en place pour assurer la confidentialité de cette clé, il est notamment conseillé de tracer les accès à cette clé. La clé secrète devra être suffisamment complexe pour ne pas affaiblir le processus d'anonymisation.*

FICHE N°10

# SÉCURITÉ DES DONNÉES

## LE CHIFFREMENT

Le chiffrement, parfois improprement appelé cryptage, est un procédé cryptographique permettant de garantir la confidentialité d'une information. D'autres mécanismes de cryptographie permettent d'assurer d'autres propriétés de sécurité, par exemple l'intégrité et l'authenticité d'un message en le signant.

De manière générale, on distingue la cryptographie symétrique où une seule clé est nécessaire (la même clé sert alors à chiffrer et à déchiffrer), de la cryptographie asymétrique dans laquelle on utilise une paire de clé : une clé publique, pouvant être connue de n'importe qui, et une clé privée dont la confidentialité doit être strictement encadrée. Dans ce deuxième cas, une clé servira à chiffrer (clé publique) et une clé secrète (différente de la clé publique) servira à déchiffrer (clé privée).

L'intérêt de la cryptographie asymétrique est multiple. Dans ce cas, chaque personne n'a besoin que d'une paire de clés privée/publique, à la différence d'un chiffrement symétrique où il est nécessaire d'avoir autant de clés différentes que de couples de personnes voulant communiquer de manière confidentielle. Cependant le chiffrement symétrique est reconnu comme étant plus rapide.

Pour identifier les algorithmes et les paramètres à utiliser en cryptographie, les annexes B1 et B2 du Référentiel Général de Sécurité peuvent être utilisées. D'un point de vue opérationnel, l'ANSSI certifie et qualifie différents produits de sécurité qui respectent, voir dépassent, ces critères.

Concernant le chiffrement symétrique, il pourra s'agir, à l'heure actuelle, d'AES avec des clés de longueur au moins égale à 128 ou 256 bits générées par des logiciels éprouvés et régulièrement mis à jour (par exemple OpenSSL). Concernant le chiffrement asymétrique, il pourrait d'agir de RSA (plus précisément celui de PKCS#1) en utilisant des modules et des clés de longueur au moins égale à 2048 bits.

### PRÉCISION

Pour les échanges intervenant entre les divers acteurs du logement social, le chiffrement des communications et des données peut s'effectuer au moyen de chiffrements symétriques ou asymétriques.

Un chiffrement symétrique permet d'utiliser une seule et même clé pour chiffrer et déchiffrer un message. Toutefois il est nécessaire d'avoir autant de clés différentes que de couples de personnes voulant communiquer de manière confidentielle. Il est également nécessaire de transmettre la clé par un vecteur de communication différent de celui utilisé pour transmettre le fichier chiffré.

Un chiffrement asymétrique nécessite une clé servant à chiffrer (clé publique) et une clé servant à déchiffrer (clé privée). Ce mode de chiffrement est intéressant lorsque les échanges interviennent entre de multiples acteurs. En effet, un message émis pourra être chiffré par la clé publique connue de tous mais ne sera déchiffrable que par les destinataires connaissant la clé privée.