

QUALITÉ DE SERVICE

Protection des
données à caractère
personnel dans les
organismes
de logement social
Guide RGPD

N°

105

Le Guide de l'Union sociale pour l'habitat sur la protection des données à caractère personnel (ci-après le « Guide RGPD » ou le « Guide ») a vocation à aider les organismes Hlm dans leur démarche de conformité pour l'application de la réglementation Informatique et Libertés (I&L).

Le cadre de référence (Livret 1) doit être lu et utilisé en combinaison avec les autres éléments du Guide RGPD de l'Union sociale pour l'habitat, notamment les référentiels (Livret 3), ainsi qu'avec les recommandations et préconisations de la CNIL.

Ce Guide RGPD est fourni à titre informatif uniquement et ne constitue pas un avis juridique. Il ne prétend pas non plus présenter des informations exhaustives, mais plutôt aider à l'appréhension des concepts et de la portée de la réglementation relative à la protection des données et des moyens pouvant être mis en œuvre par les organismes Hlm pour en assurer le respect.

Il ne remplace pas les réglementations applicables, ni les recommandations et préconisations des autorités de protection des données, dont la CNIL.

L'application des notions et des règles du RGPD a vocation à être examinée avec les services juridiques, ainsi que les délégués à la protection des données des organismes Hlm, en concertation avec les services chargés de veiller à la sécurité informatique.

PUBLICATION DE L'UNION SOCIALE POUR L'HABITAT

Pilotage et coordination

Magali Vallet, responsable du département gestion de la demande, attributions, informatique et libertés, l'Union sociale pour l'habitat

Pascal Gareau, directeur juridique et fiscal, l'Union sociale pour l'habitat

Thierry Asselin et **Delphine Baudet-Collinet**, direction des Politiques urbaines et sociale, l'Union sociale pour l'habitat

avec l'assistance de **maître Nathalie Metallinos**, Idea AARPI

Remerciements aux correspondants du réseau informatique et libertés pour leurs contributions

STRUCTURE ET CONTENU DU GUIDE RGPD

Le Guide RGPD est composé de 3 autres livrets complémentaires et interdépendants mis à disposition en version dématérialisée.

LIVRETS	CONTENU
Livret 1 Protection des données à caractère personnel dans les organismes de logement social	Cadre de référence Présentation des éléments de connaissance et de compréhension permettant aux organismes Hlm d'appréhender de manière concrète les concepts-clés de la protection des données à caractère personnel et de mettre en place leur démarche de conformité.
Livret 2	Fiches pratiques Fiches pratiques ayant vocation à préciser et illustrer les principes juridiques et répondre à des questions concrètes qui peuvent se poser aux organismes Hlm.
Livret 3	Référentiels thématiques de l'Union sociale pour l'habitat <ul style="list-style-type: none"> ● Référentiels thématiques permettent aux organismes Hlm de disposer de grilles d'analyse de conformité à la réglementation I&L. ● Reprise en le complétant et en l'actualisant du contenu des précédentes normes simplifiées et autorisations uniques du pack de conformité logement social. ● Ces référentiels ont par nature une forte composante juridique, ils présentent également une dimension pédagogique, en rappelant la nécessité de respecter certaines règles juridiques et en expliquant comment y parvenir.
Livret 4	Outils Divers outils métiers sont mis à disposition des organismes Hlm : <ul style="list-style-type: none"> ● Grille d'analyse des sous-traitants ; ● Liste des points de référence du Guide RGPD ; ● Réalisation des AIPD ; ● Exemple de formalisation des AIPD à partir des référentiels thématiques ; ● Liste type de mesures de sécurité. Ces outils constituent des modèles ou exemples à adapter par les organismes Hlm.



À NOTER

- Le présent document porte sur le Livret 1.
- Le Repères n°105 - Livret 2 est consultable via le lien suivant : <https://cahier-repere.union-habitat.org/cahier105-livret2>
- Les livrets 3 et 4 sont accessibles en version numérique gratuite sur le Centre de ressources de l'Union sociale pour l'habitat. ●



Le Guide de l'Union sociale pour l'habitat sur la protection des données à caractère personnel dans les organismes de logement social ou « Guide RGPD » :

- Constituer un guide pédagogique à destination des organismes Hlm sur l'application de la réglementation Informatique et libertés (I&L)* ;
- Refléter les évolutions légales et réglementaires ayant un impact sur le traitement* de données à caractère personnel par les organismes Hlm ;
- Proposer des solutions opérationnelles aux questions soulevées par l'application de la réglementation I&L, avec des fiches pratiques, en tenant compte de la spécificité des traitements mis en œuvre par les organismes Hlm ;
- Aider les organismes Hlm à assurer l'effectivité de l'application de la réglementation I&L.

Il est le fruit d'un travail collaboratif. L'élaboration du Guide RGPD, et plus particulièrement des fiches pratiques (livret 2) et référentiels thématiques (livret3), s'est appuyée à la fois sur :

- des groupes de travail composés d'experts internes aux organismes Hlm (directions juridiques, délégués à la protection des données, directions des systèmes d'information/responsables sécurité des systèmes d'information, responsables métiers),
- d'un comité de pilotage réuni par la Direction des Politiques urbaines et sociales de l'Union sociale pour l'habitat et associant les Fédérations Hlm, avec l'appui de la Direction Juridique et de la Direction du Numérique et des Systèmes d'information de l'Union sociale pour l'habitat¹.

Ce Guide RGPD n'a pas vocation à être exhaustif. Il porte sur 3 thématiques principales et fondamentales pour les organismes Hlm dans l'application de la réglementation I&L : la gestion de la demande, l'accompagnement social personnalisé et la gestion du patrimoine immobilier. Il ne vise pas à couvrir les traitements de données à caractère personnel en lien avec la gestion interne des organismes Hlm (gestion du personnel, gestion de la vie sociale, gestion des fournisseurs...), ni les traitements de données à caractère personnel spécifiques tels les systèmes de prise de décision automatisée. Les organismes Hlm devront s'appuyer sur les référentiels et lignes directrices de la Commission nationale de l'informatique et des libertés (CNIL) disponibles sur le site www.cnil.fr se rapportant à ces thématiques. En effet, des règles particulières, qui ne sont pas nécessairement présentées dans le présent Guide RGPD, sont susceptibles de s'appliquer à ces traitements.

* Renvoi au glossaire (Annexe A)

¹ Voir Annexe C

Le Guide RGPD n'a pas de caractère contraignant pour les organismes Hlm, contrairement à un code de conduite. Il les aide dans leur démarche de conformité en proposant une traduction des principes de protection sous forme de points de contrôle sur lesquels les organismes Hlm pourront se baser pour identifier les actions de conformité à mettre en œuvre.

Il a vocation à être régulièrement actualisé par l'Union sociale pour l'habitat. L'actualisation se fera *via* la veille postée sur l'espace collaboratif informatique et libertés et le Centre de ressources de l'Union sociale pour l'habitat, les réunions du réseau Informatique et libertés, et au fur et à mesure de l'adoption de recommandations, de modifications législatives et d'apports jurisprudentiels.



À RETENIR

Le Guide de l'Union sociale pour l'habitat sur la protection des données à caractère personnel* (ci-après le « Guide RGPD » ou le « Guide ») s'inscrit dans la continuité des précédents guides publiés par l'Union sociale pour l'habitat (guide relatif à l'application du « Pack de Conformité Logement social » de la CNIL², Guide sur la protection des données diffusé en 2017³). ●

² USH - *Repères n°1* : « Traitement des données à caractère personnel : mise en œuvre du pack de conformité logement social de la CNIL », Collection des Cahiers, octobre 2014.

³ USH, *Repères n°41* : « Règlement européen relatif à la protection des données : impacts pour les organismes Hlm », Collection des Cahiers, octobre 2017.

01

LIVRET 1

CADRE DE RÉFÉRENCE

SOMMAIRE

LIVRET 1 CADRE DE RÉFÉRENCE

07 PARTIE 1 Les principes de protection des données

- 09 Principe n°1. Justifier de l'existence d'une base légale
- 12 Principe n°2. Assurer un traitement licite, loyal et transparent
- 14 Principe n°3. Veiller à disposer d'une finalité « déterminée, explicite et légitime »
- 15 Principe n°4. Assurer le respect du principe de minimisation
- 16 Principe n°5. Veiller à l'exactitude et à la mise à jour des données
- 17 Principe n°6. Ne pas conserver les données plus que nécessaire
- 18 Principe n°7. Assurer la sécurité et la confidentialité des données
- 20 Principe n°8. Garantir le respect des droits des personnes concernées

23 PARTIE 2 Les éléments-clés de la démarche de conformité

- 25 Élément n°1. La désignation d'un DPO : pilote de la conformité
- 26 Élément n°2. La mise en œuvre de la protection des données dès la conception et de la protection des données par défaut
- 27 Élément n°3. La preuve de la conformité

30 PARTIE 3 Annexes

- 31 A - Glossaire
- 34 B - Liste des fiches pratiques du Livret 2
- 35 C - Liste des référentiels thématiques de l'Union sociale pour l'habitat du Livret 3
- 36 D - Groupes de travail et consultations en vue de l'élaboration des référentiels de l'Union sociale pour l'habitat



LÉGENDE

- * : renvoi au glossaire (Annexe A) lors de la première utilisation du mot qui y est défini
- GR n°1 : renvoi au *Repères n°1 - Traitement des données à caractère personnel, mise en œuvre du pack de conformité logement social de la CNIL – octobre 2014* - <https://www.union-habitat.org/centre-de-ressources/innovation-prospective/traitement-des-donnees-caractere-personnel-mise-en>
- GR n°2 : renvoi au *Repères n°41 - Règlement européen relatif à la protection des données : impacts pour les organismes Hlm – octobre 2017* - <https://www.union-habitat.org/centre-de-ressources/innovation-prospective/reglement-europeen-relatif-la-protection-des-donnees>
- Réf. USH-0X : renvoi à un des référentiels thématiques USH figurant dans le Livret 3
- Fiche CNIL : renvoi aux fiches sur le site de la CNIL www.cnil.fr

01

PARTIE 1

LIVRET 1

Les principes de protection des données

A - Les principes de protection des données

En vertu du principe de responsabilité ou accountability* posé à l'article 5.2 du RGPD, les organismes Hlm doivent pouvoir justifier à tout moment de leur conformité à la réglementation I&L. Les organismes Hlm sont tenus de respecter, et, le cas échéant, de faire respecter par leur sous-traitants, les principes suivants :

PRINCIPE N°1

Justifier de l'existence d'une base légale

PRINCIPE N°2

Assurer un traitement licite, loyal et transparent

PRINCIPE N°3

Veiller à disposer d'une finalité « déterminée, explicite et légitime »

PRINCIPE N°4

Assurer le respect du principe de minimisation

PRINCIPE N°5

Veiller à l'exactitude et à la mise à jour des données

PRINCIPE N°6

Ne pas conserver les données plus que nécessaire

PRINCIPE N°7

Assurer la sécurité et la confidentialité des données à caractère personnel

PRINCIPE N°8

Garantir les droits des personnes

PRINCIPE N°1. JUSTIFIER DE L'EXISTENCE D'UNE BASE LÉGALE



Des données à caractère personnel ne peuvent être recueillies et traitées par les organismes Hlm que s'ils disposent d'une base légale à cet effet, permettant le traitement.

La détermination de la base légale applicable à un traitement doit faire l'objet d'une attention particulière de la part de l'organisme Hlm.

Le choix de la base légale est une opération décisive, qui doit intervenir avant tout début de mise en œuvre du traitement des données. En l'absence de base légale, un traitement de données à caractère personnel ne peut avoir lieu. •

À titre principal, les traitements mis en œuvre par les organismes Hlm trouvent leurs fondements dans l'une des bases juridiques suivantes :

- **L'exécution d'une mission d'intérêt public dont est investi l'organisme Hlm**, tel est le cas notamment des traitements visant à assurer la sûreté et la tranquillité résidentielle, la mise en œuvre de plans d'urgence d'évacuation, ceux concourant à la mise en œuvre de l'évaluation et de l'accompagnement social personnalisé des demandeurs et locataires rencontrant des difficultés sociales, ou encore de certains traitements en rapport avec les missions d'administration des biens et missions de syndic des bailleurs.
- **Le respect des obligations légales des organismes Hlm**, notamment celles découlant de l'application du Code de la Construction et de l'Habitation. Il peut s'agir tant des traitements en lien avec la gestion de la demande de logement social (constitution du dossier, commission d'attribution, traitement des données du SNE, réalisation des enquêtes obligatoires) ou des traitements prévus par la loi, telle que l'obligation faite à tous les organismes Hlm de collecter le NIR pour le compte du ministère du logement.
- **La nécessité contractuelle**, dont notamment la conclusion et l'exécution des prestations locatives (exemple : services des eaux, entretien des immeubles), ainsi que le respect des obligations des locataires telles que visées dans le contrat de location (Exemples : la gestion des impayés locatifs, le traitement des troubles de jouissance).

De façon accessoire, les traitements sans rapport avec les missions d'intérêt public des organismes Hlm et qui ne sont pas imposés par des dispositions légales peuvent reposer sur la poursuite des intérêts légitimes de l'organisme Hlm à la condition que le traitement envisagé respecte les droits et libertés des personnes dont les règles et principes définis par le RGPD. Ainsi, les organismes Hlm mettent en œuvre des traitements visant à l'amélioration de la qualité des services, gestion des réclamations, qui peuvent notamment prendre la forme de statistiques et d'enquêtes.

De manière exceptionnelle, un traitement mis en œuvre par un organisme Hlm peut reposer sur le consentement*, lorsqu'aucun autre fondement n'est applicable et que le consentement peut être donné librement par la personne concernée (i.e. la personne doit pouvoir refuser de consentir sans que cela entraîne des conséquences négatives à son égard).



À NOTER

Les fondements applicables aux traitements visés par le Guide RGPD sont identifiés plus en détail dans chaque référentiel thématique de l'Union sociale pour l'habitat (livret 3). •

FOCUS : LA BASE LÉGALE DU TRAITEMENT DE DONNÉES SENSIBLES OU « PARTICULIÈRES »* PAR LES ORGANISMES HLM



DÉFINITION

Les données dites sensibles (données « particulières » mentionnées à l'article 9 du RGPD), sont celles relatives à l'intimité de la vie privée ; il s'agit des informations qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques à des fins d'identification unique d'une personne, les données concernant la santé*, ou concernant la vie sexuelle, ou l'orientation sexuelle d'une personne.

Leur traitement est par principe interdit. Certaines exceptions sont prévues par le RGPD et la loi Informatique et Libertés (loi I&L). Ces exceptions sont d'interprétation restrictive. Le traitement de données sensibles, lorsqu'il est permis, ne peut intervenir que moyennant la mise en œuvre de garanties renforcées destinées à assurer le respect des principes de protection des données et notamment la confidentialité et la sécurité de ces données.

À côté de ces données sensibles, les organismes Hlm doivent prêter une attention particulière au traitement de données relatives aux infractions, condamnations et mesures de sûreté qui ne peut intervenir que dans les cas prévus par la loi (sur les restrictions applicables : cf. Livret 2 / Fiche n°5). •

Cas dans lesquels les organismes Hlm traitent des données sensibles

Les organismes Hlm sont conduits à traiter des données sensibles dans plusieurs situations qui peuvent être justifiées par l'intérêt public :

- Le traitement d'informations sur le handicap des demandeurs est prévu à l'article R441-2-2 du Code de la construction et de l'habitation et est collecté via le formulaire Cerfa de la demande de logement social.
- Des données sensibles peuvent être volontairement communiquées par les intéressés eux-mêmes dans le cadre de l'évaluation sociale des demandes (cf. Réf. USH-01), dans le cadre de la gestion locative, notamment pour prendre en compte l'état de santé et/ou de dépendance résidents (Cf. réf. USH-02), l'accompagnement social personnalisé (Cf. Réf. USH-03) ou encore dans le cadre de la protection et l'assistance aux victimes et de la gestion des contentieux (cf. Réf. USH-4).

En dehors des situations en lien avec l'objectif d'intérêt général visé par la réglementation applicable aux organismes Hlm, les données sensibles n'ont pas à faire l'objet de traitement par les organismes. Certaines exceptions peuvent toutefois s'appliquer. Tel est le cas de la conduite d'enquêtes non obligatoires auprès des résidents et au cours desquelles ces derniers peuvent volontairement faire état de difficultés de santé ou de leur état de dépendance pour bénéficier de prestations ou d'accompagnement social ou dans le cas où un organisme Hlm souhaite mettre en œuvre dans le cadre de sa mission d'intérêt public une stratégie pour mieux répondre aux besoins des seniors (Cf. Réf. USH-02).

Point d'attention

À côté du régime spécial des données sensibles telles définies à l'article 9 du RGPD, les organismes Hlm doivent considérer comme sensibles dans le sens courant du terme les données suivantes (qui peuvent être qualifiées de données « hautement personnelles ») :

- données liées aux activités relevant de la vie familiale et privée ;
- identifiants nationaux tels que le NIR ;
- données concernant des personnes vulnérables (enfants, personnes âgées, personnes dépendantes) ;
- données relatives aux difficultés et évaluations sociales ;
- données relatives aux revenus ;
- données relatives aux impayés, incidents et fraudes ;
- données relatives aux moyens de paiement (RIB, numéros de cartes bancaires...) ;
- données d'évaluation (évaluation des intervenants, évaluation des besoins des locataires) ;
- ainsi que toute autre donnée dont le traitement peut avoir un impact sur l'exercice d'un droit fondamental ou dans la mesure où leur divulgation aurait clairement des incidences graves dans la vie quotidienne de la personne concernée (données financières susceptibles d'être utilisées pour des paiements frauduleux, par exemple).

Le traitement de telles données doit, tout comme celui des données sensibles de l'article 9 du RGPD, être spécifiquement justifié et être entouré de garanties spécifiques destinées notamment à assurer la confidentialité et la sécurité de ces données.

Il appartient à chaque organisme, le cas échéant, d'identifier d'autres données qui, selon son appréciation, doivent être opérationnellement traitées comme des données sensibles.

Points de contrôle*

- **C-1.** Les organismes Hlm s'assurent que les traitements qu'ils mettent en œuvre peuvent s'appuyer sur l'une des bases légales prévues à l'article 6 du RGPD, ainsi que dans la loi Informatique et libertés.
- **C-2.** Les organismes Hlm identifient les bases légales dans les notices d'information ou les politiques de protection des données personnelles mises à disposition des personnes concernées.

Bonnes pratiques

Tout changement important des conditions de mise en œuvre du traitement (finalité*, données, durées de conservation, etc.) est susceptible d'avoir une incidence sur la validité de la base légale retenue : il est donc nécessaire de réévaluer la possibilité de réaliser le traitement au regard de la base légale retenue.

Outils et références

- Guide RGPD :
 - Livret 2 / Fiche n°4 : Dans quels cas et sous quelles conditions un organisme Hlm peut-il traiter des données relatives à la santé des résidents ?
 - Livret 2 / Fiche n°5 : Dans quels cas et sous quelles conditions un organisme Hlm peut-il traiter des données relatives aux infractions, condamnations pénales et mesures de sûreté ?
 - Livret 2 / Fiche n°10 : Quel est le cadre applicable au traitement du NIR par les organismes Hlm ?
 - Livret 3 : Bases légales identifiées pour chaque activité de traitement dans chaque Référentiel thématique Union sociale pour l'habitat
- Fiches CNIL :
 - « La mission d'intérêt public : dans quels cas fonder un traitement sur cette base légale ? » (Décembre 2019)
 - « L'obligation légale : dans quels cas fonder un traitement sur cette base légale ? » (Décembre 2019)
- RGPD/I&L: art. 6 / art.5
- CEPD* :
 - Lignes directrices sur le consentement (10 avril 2018, Wp259rev.01)
 - Avis sur la notion d'intérêt légitime (9 avril 2014, Wp217)

PRINCIPE N°2. ASSURER UN TRAITEMENT LICITE, LOYAL ET TRANSPARENT



La licéité d'un traitement signifie que l'organisme Hlm est en mesure de justifier du respect de l'ensemble des exigences des dispositions légales et réglementaires applicables au traitement.

La loyauté et la transparence des traitements de données impliquent que les personnes concernées doivent être informées au préalable de manière claire et précise des données qui sont collectées et de l'usage qui en sera fait par l'organisme Hlm qui les traite conformément aux dispositions des articles 13 et 14 du RGPD.

Cette information peut se faire à plusieurs niveaux, et implique en pratique de disposer de politiques en matière de protection des données destinée à informer les personnes concernées sur leurs pratiques.

Les personnes concernées par le traitement (demandeurs, locataires, résidents...) doivent être informées des droits qui leur sont garantis par la réglementation I&L et l'organisme Hlm prend des mesures pour faciliter l'exercice de ces droits.

CONTENU DE L'INFORMATION

Information de premier niveau

L'information communiquée en première intention doit avoir pour objectif d'assurer une collecte loyale des données. Elle doit porter *a minima* sur les points suivants :

- détails de la finalité* du traitement ;
- identité du responsable du traitement ;
- description des principaux droits des personnes concernées (accès, rectification et suppression, opposition, effacement) ;
- informations sur le traitement qui aura la plus forte incidence sur la personne concernée et sur tout traitement qui pourrait la surprendre (comme le caractère facultatif ou obligatoire des données, et si la fourniture des données est prévue par les textes et lorsque la fourniture des données est obligatoire, une information sur les conséquences éventuelles d'un défaut de réponse).

Information de second niveau

Cette information doit comporter les éléments complémentaires suivants :

- coordonnées du délégué à la protection des données ;
- base juridique du traitement ;
- les destinataires* ou catégories des destinataires des données, et, le cas échéant les transferts de données en dehors de l'Union européenne et garanties applicables ;
- durée de conservation des données ;
- lorsque le traitement est fondé sur le consentement*, mention du droit de retirer son consentement à tout moment ;
- information sur les autres droits des personnes concernées : droit à la limitation* du traitement, droit d'introduire une réclamation auprès de la CNIL...
- ainsi que toute autre information utile au regard de la nature du traitement pour assurer la maîtrise par la personne concernée du traitement de ses données à caractère personnel.

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 lorsque celle-ci est nécessaire pour assurer une collecte loyale et lorsque la personne concernée en fait la demande.

Illustration : L'insertion d'une clause « informatique et libertés » dans le contrat de location est l'un des moyens pour satisfaire à l'obligation d'information. Cette clause précise l'utilisation des données à caractère personnel des locataires dans le cadre de la gestion courante (information de premier niveau). Elle renvoie, le cas échéant, à la politique de protection des données applicable au traitement des données des locataires (information de second niveau). »

Les formulaires de recueil de données à caractère personnel doivent par ailleurs comporter une mention d'information (information de premier niveau renvoyant à une information second niveau ou information complète).

Les référentiels thématiques de l'Union sociale pour l'habitat illustrent, de manière non exhaustive, différentes modalités d'information des personnes (courriers, emails, informations orales, etc.) pouvant être appliquées par les organismes Hlm.



À NOTER

Les conventions conclues en cas de mandat de gestion pourront mettre à la charge du gestionnaire l'information des personnes concernées s'agissant des traitements mis en œuvre par l'organisme Hlm. •

Point de contrôle*

- **C-3.** Existence d'une procédure interne décrivant les modalités pratiques d'information des personnes et comportant les modèles de mentions/notices à utiliser

Bonnes pratiques

- Assurer l'information des locataires via une mention du contrat de location (premier niveau d'information) renvoyant à une notice plus complète accessible facilement (deuxième niveau d'information). À défaut, remise au locataire d'un document séparé contre signature lors de la signature du contrat de location.
- Intégrer les notices/mentions d'information dans une politique de protection des données de l'organisme Hlm directement accessible depuis le site web institutionnel de l'organisme Hlm ou les extranets dédiés (extranet locataires, extranet fournisseurs...).
- Recourir à des icônes ou des infographies pour faciliter la compréhension des notices.

Outils et références

- Guide RGPD :
 - Livret 2 / Fiche n°7 : Comment assurer en pratique la transparence sur les traitements ?
 - Livret 3 : Modalités d'information identifiées pour chaque activité de traitement dans chaque référentiel de l'Union sociale pour l'habitat.
 - Livret 4 : Modèle de clause à insérer dans le bail/mentions-types.
- RGPD : art.5. 1 a et art. 12 à 14.
- CEPD : Lignes directrices sur la transparence du 11 avril 2018 (Wp260rev.01).

PRINCIPE N°3. VEILLER À DISPOSER D'UNE FINALITÉ « DÉTERMINÉE, EXPLICITE ET LÉGITIME »



Des données à caractère personnel ne peuvent être recueillies et traitées par les organismes Hlm que pour un usage déterminé, explicite et légitime, dans la mesure nécessaire à leurs missions et dans la limite permise par les bases légales identifiées.

La finalité doit avoir été déterminée préalablement à la collecte et les personnes concernées doivent en être informées de manière claire et accessible afin de leur permettre d'identifier l'étendue du traitement et les conséquences à leur égard.

La compatibilité de la finalité du traitement avec la base légale envisagée doit avoir été vérifiée par l'organisme Hlm. Les données à caractère personnel collectées pour une finalité donnée ne doivent pas être traitées ultérieurement de manière incompatible avec la finalité initiale.●

Les référentiels thématiques de l'Union sociale pour l'habitat présentent les objectifs généralement poursuivis par les organismes Hlm.

USAGE COMPATIBLE	INFORMATION SUR LES FINALITÉS
<p>Pour déterminer si la finalité est compatible, il est nécessaire de tenir compte :</p> <ul style="list-style-type: none"> ● du lien entre la finalité initiale et les finalités du traitement ultérieur prévu ; ● du contexte dans lequel les données à caractère personnel ont été collectées, en particulier les attentes raisonnables des personnes concernées, en fonction de leur relation avec le responsable du traitement ; ● de la nature des données à caractère personnel ; ● des conséquences pour les personnes concernées du traitement ultérieur prévu ; ● de l'existence de garanties appropriées à la fois dans le cadre du traitement initial et du traitement ultérieur prévu. 	<p>Les personnes concernées doivent être informées de manière claire et précise sur les finalités poursuivies dans un langage accessible.</p> <p>L'information peut être effectuée de manière autonome (envoi d'un courrier ou d'une lettre circulaire, déplacement au domicile des personnes, appel téléphonique...) ou être réalisée à l'occasion d'un autre événement notamment pour rationaliser les coûts (enquête sur l'occupation du parc social, autre enquête obligatoire...).</p> <p>Dans ce dernier cas, les résidents doivent être clairement informés des deux finalités distinctes poursuivies par l'organisme Hlm (par exemple : réalisation d'une enquête obligatoire, mise à jour des données de leur dossier), ainsi que du caractère obligatoire ou facultatif des réponses et des conséquences qui peuvent en résulter.</p>

EXEMPLE D'USAGE NON COMPATIBLE

Un fichier* qui concerne les dossiers des résidents d'un ensemble immobilier ne doit servir qu'à la gestion de la relation entre l'organisme Hlm et les occupants de son parc. Ces informations ne peuvent ainsi être utilisées à des fins de prospection commerciale au profit d'un tiers (exemple : promoteur privé) ou à des fins politiques.

Point de contrôle*

- **C-4.** Les organismes Hlm s'assurent que les traitements qu'ils mettent en œuvre répondent à une finalité préalablement identifiée et légitime. Toute utilisation des données pour une autre finalité doit faire l'objet d'une analyse de compatibilité par l'organisme Hlm

Outils et références

- Guide RGPD USH :
 - Livret 3 : Référentiels thématiques de l'Union sociale pour l'habitat, finalités identifiées pour chaque activité de traitement dans chaque référentiel thématique de l'Union sociale pour l'habitat.
- RGPD : art.5. 1 b
- CEPD : Avis du G29 sur la limitation de la finalité, 2 avril 2013)⁴.
- Fiche CNIL : « Définir une finalité »

⁴ Disponible en anglais uniquement

PRINCIPE N°4. ASSURER LE RESPECT DU PRINCIPE DE MINIMISATION



La minimisation* consiste à s'assurer que les données à caractère personnel collectées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles seront traitées.

Les référentiels thématiques Union sociale pour l'habitat identifient des catégories de données en lien avec les différentes activités de traitement concernées par le présent Guide.●

L'organisme Hlm privilégie en toutes circonstances la collecte de données la moins intrusive pour la vie privée.

Le fait qu'une donnée dont la collecte soit visée par l'un des référentiels thématiques de l'Union sociale pour l'habitat ne signifie pas qu'elle doive être systématiquement collectée.

L'organisme Hlm doit pouvoir justifier au cas par cas du bien-fondé de la collecte de chaque catégorie de données au regard de la finalité du traitement et de la situation individuelle de la personne concernée, qu'elle soit ou non visée dans un référentiel thématique Union sociale pour l'habitat : la collecte doit être réellement utile pour atteindre la finalité. Il n'est pas possible de collecter toutes les données, pour ensuite faire le tri.

Par exemple : ne pas collecter une pathologie sans incidence sur le logement et la sécurité de la personne.

Dans le cadre de la gestion des rapports locatifs, la nature du handicap d'un résident ne doit être renseignée que si cette information a une incidence sur les caractéristiques du logement ou appelle des modalités particulières de traitement en cas de sinistre (exemple d'une personne lourdement handicapée en cas

d'incendie), et sous réserve qu'il ne soit pas possible de se limiter à la collecte d'une donnée plus générale, et d'une restriction du nombre de personnes autorisées à accéder à cette information (principe du besoin d'en connaître*).

La minimisation peut également résulter de mesures telles que la pseudonymisation* ou l'anonymisation*, ou encore la limitation de la durée de conservation des données.

Points de contrôle

- C-5. Être en mesure de justifier de la légitimité et du caractère strictement nécessaire de la collecte des données à caractère personnel au regard de la finalité du traitement.
- C-6. Existence d'une procédure interne rappelant les cas et conditions dans lesquels des données sensibles (santé, perte d'autonomie, difficultés sociales, infractions, condamnations pénales et mesures de sûreté) peuvent être traitées par l'organisme Hlm.

Outils et références

- Guide RGPD Livret 2 :
 - Fiche n°2 : Quelles sont les règles applicables à l'utilisation des champs libres et zones de commentaires ?
 - Fiche n°3 : Quelles sont les règles à appliquer au traitement d'appréciations sur les difficultés sociales des personnes par les organismes Hlm ?
 - Fiche n°4 : Dans quels cas et sous quelles conditions un organisme Hlm peut-il traiter de données relatives à la santé des résidents ?
 - Fiche n°5 : Dans quels cas et sous quelles conditions un organisme Hlm peut-il traiter des données relatives aux infractions, condamnations pénales et mesures de sûreté ?
 - Fiche n°6 : Quelles précautions en cas de traitement des données à caractère personnel relatives aux enfants ?

-Fiche n°10 : Quel est le cadre applicable au traitement du NIR par les organismes Hlm ?

-Fiche n°11 : Comment assurer la réalisation d'enquêtes en conformité avec le RGPD ? : enquêtes obligatoires et facultatives.

- RGPD : art. 5. 1 c).
- CEPD : Lignes directrices 4/2019 sur l'Article 25 « Protection des données dès la conception et par défaut », adopté le 13 Novembre 2019
- Fiches CNIL : Minimiser les données collectées et vérifier la pertinence des données

PRINCIPE N°5. VEILLER À L'EXACTITUDE ET À LA MISE À JOUR DES DONNÉES



Les organismes Hlm sont tenus d'assurer l'exactitude et la mise à jour des données à caractère personnel traitées eu égard aux finalités pour lesquelles elles sont traitées. Le cas échéant, les données qui sont inexactes doivent être effacées ou rectifiées sans tarder. •

L'organisme Hlm doit prendre toutes les mesures appropriées pour s'assurer que les données personnelles conservées ne sont pas inexactes ou erronées concernant la situation des personnes concernées, il est à ce titre important pour les organismes Hlm d'assurer la mise à jour du dossier des locataires à l'occasion de l'enquête OPS.

L'exactitude des données est ainsi assurée à divers niveaux :

- Les données relatives aux locataires et résidents sont mises à jour à la suite des enquêtes obligatoires (enquêtes OPS) ;
- Concernant les demandeurs, les données des dossiers de demande de logement social (comme les informations relatives aux ressources, les indicateurs de suivi...) sont mises à jour via le SNE et vérifiées préalablement au passage en Commissions d'attribution des logements et d'examen de l'occupation des logements (CALEOL).

L'organisme Hlm corrige par ailleurs les données à caractère personnel dès qu'il a connaissance de leur inexactitude, notamment dans le cadre des réclamations adressées par les personnes concernées.

Dans le cadre d'une prise de décision, l'organisme Hlm doit, par ailleurs, s'assurer que les données à caractère personnel utilisées ont été mises à jour.

Point de contrôle

- **C-7.** Mettre en place une procédure permettant d'identifier les catégories de données devant faire l'objet de mises à jour régulières et les modalités applicables, ainsi que la bonne prise en compte de l'exercice du droit de rectification des personnes concernées (demandeurs, locataires, résidents...)

Outils et références

- Guide RGPD :
 - Livret 3 : Mesures proposées dans les référentiels thématiques pour assurer la mise à jour des informations
- RGPD : art. 5.1 d), art.16 et 17 (rectification et effacement)

PRINCIPE N°6. VEILLER À L'EXACTITUDE ET À LA MISE À JOUR DES DONNÉES



Les organismes Hlm sont amenés à collecter de nombreuses données sur les demandeurs de logement social, les résidents ou des personnes intervenant sur le parc immobilier. Ces données à caractère personnel ne peuvent être conservées de façon indéfinie dans un fichier* ou un système de traitement.

Une durée de conservation doit impérativement être déterminée, en fonction de la finalité de chaque fichier ou traitement, par l'organisme Hlm. •

Une durée de conservation peut renvoyer à une durée fixe exprimée en jours, en mois ou en années ou également s'exprimer par référence à un événement butoir (durée du contrat de location, durée d'instruction de la demande...).

Il faut distinguer la durée de conservation en base active ou archives courantes, de la durée d'archivage intermédiaire et de l'archivage définitif.

Au-delà de la durée nécessaire aux finalités de la collecte (archives courantes), les données strictement nécessaires à l'accomplissement d'obligations légales peuvent faire l'objet d'un archivage intermédiaire le temps nécessaire au respect de l'obligation en cause ou à des fins probatoires en cas de contentieux pendant la durée de la prescription applicable.

À l'expiration de ces délais, les données sont supprimées ou anonymisées ou archivées dans les conditions prévues par les dispositions du Code du patrimoine prescrivant aux gestionnaires publics de logement sociaux de verser des documents au service d'archivage départemental⁵.

La conservation et l'archivage des données doivent être réalisés dans des conditions de sécurité conformes aux dispositions de l'article 32 du RGPD.

⁵ Applicable à tous les organismes Hlm

Points de contrôle

- **C-8.** L'organisme Hlm doit documenter les règles définies en matière de durée de conservation et d'archivage.
- **C-9.** L'organisme Hlm doit transcrire dans les processus métiers les mesures, notamment techniques, permettant d'assurer le respect des règles de conservation définies.

Outils et références

- Guide RGPD :
 - Livret 2, Fiche n°9 : Comment définir le cycle de vie des données ?
 - Livret 3 : Durées de conservation proposées dans chaque référentiel thématique USH
- CNIL : Guide pratique sur les durées de conservation (2020)
- RGPD : art. art. 5. 1^{er})



ILLUSTRATION

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 à l'organisme Hlm. 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.

Ainsi, les données à caractère personnel se rapportant aux dossiers instruits en Commissions d'attribution des logements et d'examen de l'occupation des logements (CALEOL) sont conservées pendant une durée de six ans (cinq années correspondant à la périodicité des contrôles + 1 an) aux fins de permettre la réalisation des contrôles de l'Agence nationale du contrôle du logement social (ANCOLS). •

PRINCIPE N°7. ASSURER LA SÉCURITÉ ET LA CONFIDENTIALITÉ DES DONNÉES



La sécurité des données à caractère personnel est un volet essentiel de la conformité à la réglementation I&L.

Les données à caractère personnel doivent être traitées de façon à garantir un niveau de sécurité approprié desdites données, et les protéger contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles.

Les organismes Hlm doivent donc mettre en place (et veiller à ce que leurs sous-traitants mettent en place) des pratiques et des mesures destinées à identifier, estimer et traiter les risques.

En application du principe de responsabilité, l'organisme Hlm devra démontrer (et le cas échéant devra obtenir du sous-traitant qu'il démontre) le respect de l'exigence de sécurité. •

L'identification des mesures de sécurité

Les mesures de sécurité tiennent compte :

- De l'état des connaissances ;
- Des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ;
- Des risques pour les droits et libertés des personnes physiques.

Elles doivent permettre à l'organisme Hlm d'assurer le respect de l'obligation de discrétion et de secret professionnel ⁶.

⁶ En plus de l'obligation de discrétion professionnelle à laquelle sont tenus tous les personnels des organismes Hlm, certains personnels sont tenus, en raison de leurs fonctions ou des missions qui leur sont confiées, au secret professionnel ; tel est le cas des travailleurs sociaux (article L411-3 du code de l'action sociale et des familles), des membres de la commission de coordination des actions de prévention des expulsions (CCAPEX), ainsi que des personnes chargées de l'instruction des saisies ou participant aux commissions/sous-commissions (article 7-2 de la loi n° 90-449 du 31 mai 1990 visant à la mise en œuvre du droit au logement modifié par la loi ALUR n°2014-366 du 24 mars 2014 - art. 28 et décret n° 2015-1384 du 30 octobre 2015 relatif à la commission de coordination des actions de prévention des expulsions locatives) ; les membres de la commission de médiation DALO et les personnes chargées de l'instruction de sa saisine (article L441-2-3 du Code de la construction et de l'habitation) ; les personnes qui accompagnent la personne âgée en perte d'autonomie suivant la méthode d'action pour l'intégration des services d'aide et de soins dans le champ de l'autonomie (MAIA) (art.113-3 du code de l'action sociale et des familles).

L'organisme Hlm doit :

- S'assurer de l'efficacité des moyens humains, organisationnels et techniques mis en œuvre pour assurer la sécurité des données ;
- S'assurer que les données à caractère personnel ne sont pas divulguées à des tiers non autorisés.

La sécurité encadrant la communication des données à des tiers

Avant de communiquer des données à un organisme extérieur, un organisme Hlm doit ainsi se poser un certain nombre de questions, en particulier quant au respect des droits des résidents.

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

Dans ce cas, l'organisme Hlm s'assure du caractère obligatoire du texte utilisé à l'appui de la demande de l'organisme tiers, et ne transmet 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.

La sécurité du recours à la sous-traitance

En cas de sous-traitance, le sous-traitant et, le cas échéant le sous-traitant ultérieur, doivent garantir qu'ils ne traitent les données à caractère personnel que sur instructions du responsable de traitement. Pour cela il faut s'en assurer par le biais de clauses contractuelles ou la mise en place d'audits.

Point de contrôle

- **C-10.** Vérifier que les mesures de sécurité applicables à chaque traitement sont appropriées et documentées

Bonnes pratiques

- Aller progressivement vers la formalisation d'une politique Sécurité des Systèmes d'Information (SSI) ;
- Disposer d'une procédure de rédaction d'une « fiche de sécurité » d'un projet informatique destinée à identifier et évaluer les points particuliers de sécurité d'un projet ;
- Faire figurer les éléments principaux relatifs à la sécurité des traitements ou de l'existence de la documentation s'y rapportant et de sa localisation dans le cadre de la tenue de la cartographie des traitements.

Outils et références

- Référentiels thématiques de l'Union sociale pour l'habitat :
 - Livret 2, Fiche pratique n°8 : Comment organiser et gérer la sécurité des traitements ?
 - Livret 3 : Mesures de sécurité générales et spécifiques proposées dans les référentiels de l'Union sociale pour l'habitat
- RGPD : art. Art. 5. 1 f).; art. 28 à 33.
- CNIL :
 - Dossier cybersécurité de la CNIL <https://www.cnil.fr/fr/cybersecurite>
 - Guide de la sécurité des données personnelles, 23 janvier 2018

- Guide pratique « tiers autorisés » et « Recueil des procédures tiers autorisés », juillet 2020
- Fiche CNIL : 10 conseils pour la sécurité de votre système d'information, 12 octobre 2009
- La partie « étude des risques de sécurité » des guides et du logiciel libre de la CNIL pour mener des PIA
- Délibération n° 2021-122 du 14 octobre 2021 portant adoption d'une recommandation relative à la journalisation

Autres ressources

- Guide des bonnes pratiques de l'informatique ANSSI-CPME
- Guide d'hygiène informatique de l'ANSSI (Version 2.0 - Septembre 2017)
- Normes ISO 31000 (gestion des risques) - ISO/IEC 27001 (exigences pour un système de management de la sécurité de l'information) - ISO/IEC 27005 (gestion des risques de sécurité de l'information)

PRINCIPE N°8. GARANTIR LE RESPECT DES DROITS DES PERSONNES CONCERNÉES



Le RGPD garantit un certain nombre de droits aux personnes concernées.

La prise en compte de ces droits par les organismes Hlm doit être une préoccupation constante des organismes Hlm qui doivent mettre en place toutes les mesures techniques et organisationnelles permettant d'en garantir le respect. •



Le droit d'accès et de copie

Permet à la personne concernée, sauf disposition législative ou réglementaire contraire, d'interroger l'organisme Hlm sur le traitement de données à caractère personnel la concernant, de les visualiser et les vérifier et d'en obtenir une copie ; ce droit concerne également les résultats de combinaisons, calculs et rapprochements (comme un score de recouvrement ou un « scoring » utilisé pour préciser les attributions).

Un résident doit pouvoir à tout moment avoir accès et obtenir, sur simple demande, la communication d'une copie de toutes les données le concernant et figurant dans les différents fichiers de l'organisme Hlm (dossier individuel, zones de commentaires, enregistrements vidéo...), y compris les données archivées. L'organisme Hlm doit s'assurer de ne pas rendre accessibles ou de ne pas communiquer de données à caractère personnel de tiers. Il convient de flouter ou couper des parties d'enregistrements vidéo pour rendre les tiers non identifiables.

La personne concernée doit pouvoir avoir accès à l'origine des données lorsque les données à caractère personnel n'ont pas été collectées directement auprès d'elle et notamment si elles proviennent d'une source publique.

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

L'organismes Hlm peut ne pas donner suite à la demande de droit d'accès si la demande est infondée ou excessive, à condition d'être en mesure d'apporter la preuve de ce caractère « infondé » ou « excessif ».

Droit de rectification et de suppression

Ce droit permet à la personne concernée de modifier et/ou compléter les données à caractère personnel la concernant qui sont inexactes ou incomplètes. L'exercice de ce droit est complémentaire à l'obligation de l'organisme Hlm d'assurer l'exactitude, et si besoin la mise à jour des données à caractère personnel qu'il traite. L'organisme Hlm doit satisfaire la demande dans les meilleurs délais et au maximum sous un mois.

Exemple : le dossier de demande de logement social enregistré sur le SNE ou le SPTA mentionne par erreur qu'un demandeur est célibataire, l'organisme Hlm doit opérer la rectification dans les plus brefs délais dans la mesure où cette erreur peut entraîner des conséquences sur la décision d'attribution d'un logement.

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

Le droit à l'effacement

Ce droit permet à la personne concernée de demander la suppression de ses données à caractère personnel dans les cas suivants :

- La personne concernée considère que le traitement de ses données à caractère personnel par l'organisme Hlm n'est plus nécessaire au regard des finalités pour lesquelles elles ont été collectées ou traitées ou que leur conservation est contraire à la loi.



À NOTER

Nonobstant l'exercice du droit à l'effacement ou à la limitation, l'organisme Hlm peut conserver certaines données à caractère personnel. C'est le cas lorsque la loi l'impose ou l'autorise. C'est le cas lorsque l'organisme Hlm justifie d'un motif légitime de le faire (par exemple pour justifier de l'exécution d'un contrat), pour l'exercice ou la défense de droits en justice ou encore lorsque l'exercice du droit d'effacement porte atteinte à droit à la liberté d'expression et d'information. ●

Exemple : la personne ne souhaite plus faire l'objet d'un accompagnement social personnalisé et demande par conséquent la suppression des données collectées dans ce cadre de la base active de l'organisme Hlm. L'exercice de ce droit ne fait pas obstacle à la conservation de certaines données en archives à des fins probatoires.

- La personne concernée a retiré son consentement au traitement de ses données à caractère personnel.

Exemple : un résident s'étant inscrit sur une liste pour recevoir une « newsletter » peut à tout moment notifier son souhait de ne plus figurer sur la liste de diffusion.

- La personne concernée s'oppose au traitement de ses données à caractère personnel pour des motifs tenant à sa situation personnelle.

Exemple : il est fait état dans son dossier de locataire d'un trouble de voisinage dont il a été l'auteur plus de 8 ans auparavant, et aucun autre trouble ne lui est imputable depuis : le résident est en droit de demander l'effacement de la base active de cette référence qui porte sur des faits anciens et dont le maintien est susceptible de porter atteinte à sa réputation.

Droit à la portabilité

Ce droit permet, sous certaines conditions, à la personne concernée de recevoir les données à caractère personnel qu'elle a fournies à l'organisme Hlm, dans un format structuré couramment utilisé, lisible par machine et interopérable et d'obtenir, lorsque cela est techniquement possible, la transmission de ces données à un tiers qu'elle aura désigné. Ce droit ne s'exerce que lorsque la base légale du traitement est le consentement de la personne concernée ou l'exécution d'un contrat et que les données ont été directement fournies par la personne concernée de manière entièrement automatisée.

Exemple : un résident a créé un compte en ligne lui permettant de poster des commentaires dans un forum de résidents proposé par l'organisme Hlm : le droit à la portabilité s'exerce sur les commentaires qu'il a postés.



À NOTER

Le droit à la portabilité ne s'applique pas aux données collectées dans le cadre de la gestion de la demande ou aux fins du suivi personnalisé des personnes. Ce droit ne s'applique que pour les traitements reposant sur le consentement ou lorsque le traitement est nécessaire pour l'exécution d'un contrat. Il devrait donc être d'application très limitée pour les organismes Hlm. ●

Droit d'opposition

L'exercice du droit d'opposition permet à la personne concernée de s'opposer à la collecte ou la conservation de données complémentaires non prévues par la loi.

Le droit d'opposition s'applique si le traitement est fondé sur l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, ou fondé sur l'intérêt légitime du responsable de traitement.

La personne concernée ne peut pas s'opposer au traitement lorsqu'il est prévu par la loi ou lorsqu'il est nécessaire pour répondre à une obligation légale à laquelle l'organisme Hlm est tenu.

C'est à l'organisme Hlm de justifier de l'existence d'un motif légitime impérieux pour continuer à traiter les données et non à la personne concernée de justifier d'un intérêt légitime pour exercer son droit d'opposition.

Par ailleurs, un résident est en droit de s'opposer, à tout moment et sans conditions, à ce que des données le concernant soient utilisées à des fins de sollicitations, notamment commerciale.

Droit à la limitation du traitement

Ce droit permet à la personne concernée de demander à l'organisme Hlm, à la place de l'effacement, le gel temporaire de ses données à caractère personnel.

Exemple : une personne concernée demande à un organisme Hlm de verrouiller les images du système de vidéosurveillance le temps nécessaire pour exercer un recours et demander la production des images en justice.

Désignation du service chargé de recevoir les demandes d'exercice de droit des personnes concernées

L'organisme Hlm doit désigner un service auprès duquel s'exercent directement les droits des personnes concernées ; ce service peut différer selon les catégories de personnes concernées. L'organisme Hlm met en œuvre toute autre mesure destinée à faciliter l'exercice des droits des personnes, comme une adresse de courriel dédiée.

Délai d'instruction des demandes

L'organisme Hlm dispose d'un délai d'un mois pour répondre à une demande d'exercice de droit d'une personne. Ce délai peut être prorogé de deux mois supplémentaires en cas de complexité de la demande. Le cas échéant, l'organisme Hlm doit informer le demandeur de cette prolongation dans le délai initial d'un mois.

La vérification de l'identité du demandeur

Un organisme Hlm doit vérifier l'identité de la personne concernée avant une

demande d'exercice de ses droits. S'il est légitime que l'organisme Hlm demande des informations nécessaires pour assurer l'identification certaines de la personne concernée, la demande de production de justificatifs d'identité officiels (carte d'identité, passeport) ne peut être systématique. Elle ne doit intervenir que lorsque les informations communiquées par la personne concernée ne permettent pas de lever tout doute sur son identité ou en raison de la sensibilité des données.

Droit à réclamation

Les personnes concernées disposent également du droit de saisir la Commission nationale de l'informatique et des libertés (CNIL) de toute réclamation concernant le traitement de leurs données à caractère personnel.

Point de contrôle

C-11. L'organisme Hlm doit avoir identifié dans une procédure interne les modalités de traitement des demandes d'exercice des droits des personnes concernées ; cette procédure doit permettre une information suffisante des services internes de l'organisme Hlm sur l'étendue des droits des personnes concernées,

ainsi que sur les délais de réponse prescrits par la réglementation I&L et le RGPD.

Bonnes pratiques

- Développer et mettre à disposition des personnes concernées des formulaires dédiés à l'exercice des droits des personnes.
- Veiller à ce que les données à caractère personnel d'une personne puissent être rapidement et facilement identifiées dans le système d'information : la tenue du registre ainsi que la cartographie des traitements (v. infra 4.1) est à cet égard l'un des moyens permettant de localiser rapidement les données à caractère personnel.

Références utiles

- Référentiels thématiques de l'Union sociale pour l'habitat :
 - Livret 3 : Point 9. Droit des personnes de chaque référentiel
- CNIL :
 - Fiche pratique : « Respecter les droits des personnes » : <https://www.cnil.fr/fr/respecter-les-droits-des-personnes>



PRÉCISION

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 organisme Hlm qu'il prenne en compte ce décès et mette à jour son traitement.

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

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. ●

02

PARTIE 1

LIVRET 1

Les éléments-clés de la démarche de conformité

Les organismes Hlm doivent pouvoir démontrer la conformité de leurs activités de traitement de données à caractère personnel avec le RGPD. Cette obligation porte non seulement sur l'existence des mesures destinées à assurer la conformité, mais également sur leur efficacité au regard des risques identifiés pour les droits et libertés des personnes concernées. Elle implique la mise en place d'un programme de conformité.

Les organismes Hlm doivent intégrer dans leur programme de conformité la prise en compte de la protection des données dès la conception* (« privacy by design ») et par défaut* (« privacy by default ») de tout traitement comportant des données à caractère personnel.

Sur l'ensemble de ces aspects, le délégué à la protection des données joue un rôle-clé. Sa désignation est donc à bien des égards la première action de conformité à mettre en œuvre.

ELÉMENT N°1

La désignation d'un DPO : pilote de la conformité

ELÉMENT N°2

La protection des données dès la conception et par défaut

ELÉMENT N°3

La preuve de la conformité

ÉLÉMENT N°1. LA DÉSIGNATION D'UN DPO : PILOTE DE LA CONFORMITÉ

Les délégués à la protection des données (DPO) jouent un rôle majeur pour assurer le respect effectif des principes de protection des données dans les organismes Hlm. Pour garantir le respect du droit fondamental à la protection des données, un engagement de la direction de l'organisme Hlm est nécessaire. Les personnes concernées doivent être informées de la désignation du DPO, ainsi que de ses coordonnées.

Les missions du DPO au sein de l'organisme Hlm

Les missions du DPO ont été précisées dans des lignes directrices adoptées par le Comité européen sur la protection des données (CEPD), ainsi que par la CNIL :

- Informer et conseiller le Directeur général en sa qualité de responsable de traitement ;
- Contrôler le respect du RGPD et de la loi Informatique et libertés ;
- Conseiller l'organisme Hlm sur la réalisation d'une analyse d'impact relative à la protection des données et en vérifier l'exécution ;
- Coopérer avec la CNIL et être son point de contact ;
- Tenir compte, dans l'accomplissement des missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Avant de désigner un(e) DPO, l'organisme Hlm vérifie qu'il(elle) dispose du statut, des compétences et des moyens nécessaires à l'exercice de ses missions.

Sa désignation doit être notifiée à la CNIL.

Statut

Le DPO peut être interne à l'organisme Hlm ou externalisé⁷. Il peut également être mutualisé⁸ avec un autre organisme Hlm. En cas d'externalisation ou de mutualisation, l'organisme Hlm doit s'assurer que le DPO reste facilement joignable à partir de chaque établissement de l'organisme Hlm et suffisamment proche pour exercer convenablement ses missions.

La personne désignée en qualité de DPO n'exerce pas nécessairement ses fonctions à plein temps et, selon la taille et l'organisation interne de l'organisme Hlm, ses fonctions peuvent être confiées à une « équipe DPO » (le DPO et juristes et /ou informaticiens qui l'appuient dans ses fonctions).

Compétences et expertise du DPO

- Expertise relative aux législations nationale et européenne en matière de protection des données, y compris une connaissance approfondie du RGPD ;
- Compréhension des opérations de traitement effectuées ;
- Compréhension des technologies de l'information et de la sécurité des données ;
- Connaissance du secteur d'activité et de l'organisme ;
- Capacité à promouvoir une culture de protection des données au sein de l'organisme.

Responsabilité de la direction générale de l'organisme Hlm

- Doter le DPO de moyens matériels adéquats (adresse e-mail dédiée, espace dédié dans l'intranet...) ;
- S'assurer que le DPO est à l'abri des conflits d'intérêts en veillant à ce que les tâches de DPO sont compatibles avec les autres responsabilités qui lui sont confiées ;
- Proposer au DPO des formations relatives à la protection des données ;
- Permettre au DPO de mener des actions de communication interne auprès du personnel, par le biais de communiqués, de l'intranet, de brochures, de stages ;
- Veiller à ce que le DPO soit consulté préalablement à la mise en œuvre de tout nouveau traitement ;
- Assurer la continuité de la fonction.

Points de contrôle

C-12. L'organisme Hlm a désigné un délégué à la protection des données (DPO) disposant des compétences visées au Chapitre IV Section 4 du RDPG.

C-13. Les coordonnées du DPO sont communiquées aux personnes concernées

(figurent dans les mentions d'informations sur les formulaires de recueil de données, sites internet, etc.).

Bonnes pratiques

- Si l'organisation le permet, désignation d'un DPO adjoint afin d'assurer la continuité de la fonction en cas d'arrêt, d'absence prolongée du DPO (congé maladie, maternité...) ou à défaut désigner un DPO par intérim.
- Identification par le DPO des critères d'évaluation du bon fonctionnement de la fonction de DPO (programme de travail annuel, exigences quant à l'entretien des connaissances...).

Outils & références

- Circulaire de l'Union sociale pour l'habitat n°31/18 : « Mise en œuvre du règlement européen relatif à la protection des données »
- RGPD : art. 37 à 39
- G29/CEPD : Lignes directrices du Groupe de l'article 29 concernant les délégués à la protection des données (DPD), adoptées le 13 décembre 2016 et révisées et adoptées le 5 avril 2017 [WP 243 rev.01]
- CNIL :
 - Le guide pratique des DPO
 - Référentiel de certification des DPO de la CNIL (Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO))
- Téléservice de désignation du DPO : <https://designations.cnil.fr/dpo/designation/organisme.designant.delegue.action>

⁷ Le DPO est alors un prestataire de services, externe à l'organisme Hlm, lié par un contrat de prestation des services.

⁸ Un même DPO exerçant ces fonctions au sein de plusieurs organisme Hlm

ÉLÉMENT N°2. LA MISE EN ŒUVRE DE LA PROTECTION DES DONNÉES DÈS LA CONCEPTION ET DE LA PROTECTION DES DONNÉES PAR DÉFAUT

Protection dès la conception

Le volet protection des données dès la conception ou « privacy by design » concerne la mise en place d'une protection dès la création du système d'information ou du traitement, et ce, tout le long des traitements.

Il s'agit donc pour les organismes Hlm :

- De réfléchir à la problématique des données personnelles lors de la mise en place d'un nouveau projet ;
- D'envisager des règles et des procédures permettant d'assurer la protection de ces données et la conformité au RGPD dès la conception ;
- D'imposer à leurs prestataires et sous-traitant de prendre en compte des principes de protection des données dès la conception dans le cadre du développement des outils informatiques.

Ces exigences peuvent se traduire par des choix d'architecture (décentralisée vs. centralisée), de fonctionnalités (anonymisation à bref délai, minimisation des données, purge automatique, outils de gestion fine des droits et habilitations), de technologies (chiffrement des communications).



À RETENIR

L'implémentation de ces règles constitue l'un des éléments permettant au responsable de traitement de démontrer sa conformité et participe à la bonne mise en œuvre du principe « d'accountability ». •

Protection par défaut

La protection des données par défaut complète idéalement la protection dès la conception ou dans certains cas pallie son absence. Elle consiste à paramétrer les outils et applications *a posteriori*, dans un sens assurant le plus haut niveau de protection.

L'objectif de la protection par défaut est atteint dès lors que la personne concernée n'a aucune action à entreprendre pour que ses données et ses droits soient respectés (exemple : la mise en place d'un système de purge obligatoire s'activant périodiquement).

Point de contrôle

C-14. Identification, pour chaque traitement, des mesures et procédures techniques et organisationnelles appropriées afin d'assurer la conformité à la réglementation I&L.

Bonnes pratiques

- Assurer l'intégration des concepts clés du RGPD dans le parcours utilisateur des téléservices à destination des résidents ;
- Faciliter l'exercice du droit d'accès en prévoyant des requêtes permettant d'extraire l'ensemble des données se rapportant à un résident ;
- Choisir des solutions informatiques permettant une gestion fine des droits d'accès et habilitations ;
- Choisir des solutions informatiques intégrant des fonctions d'archivage et de suppression automatiques ;
- Choisir des formats de saisie et d'enregistrement des données qui minimisent les données collectées (exemple : âge plutôt que date de naissance) ;
- Éviter le recours à des zones de texte libre ou de commentaires.

Outils et références

- RGPD : art. 25
- G29/CEPD : Lignes directrices 4/2019 sur l'article 25 « protection dès la conception et par défaut », adopté le 13 novembre 2019
- CNIL :
 - Guide RGPD du développeur, 13 mai 2019
 - Guide La sécurité des données personnelles
 - Fiches CNIL :
 - Prendre en compte les bases légales dans l'implémentation technique, 27 janvier 2020
 - Préparer l'exercice des droits des personnes, 27 janvier 2020
 - Sécurité : Encadrer les développements informatiques : <https://www.cnil.fr/fr/securite-encadrer-les-developpements-informatiques>
 - Organiser les processus internes, 23 août 2018 : <https://www.cnil.fr/fr/organiser-les-processus-interne>
 - RGPD en pratique : communiquer en ligne : <https://www.cnil.fr/fr/rgpd-en-pratique-communiquer-en-ligne>
 - Mini site CNIL « Données & Design par Linc » : <https://design.cnil.fr/>

ÉLÉMENT N°3. LA PREUVE DE LA CONFORMITÉ



L'obligation de démontrer la conformité des traitements impose à l'organisme Hlm de disposer de politiques et procédures à l'appui du programme de conformité à la réglementation I&L. Il doit également assurer le contrôle et la vérification de l'efficacité de l'organisation et des règles tout au long de leur mise en œuvre.

Ces politiques et procédures doivent être rédigées après avis du délégué à la protection des données qui doit être en mesure d'en contrôler le respect. Elles sont régulièrement réexaminées et actualisées si nécessaire. •

L'existence d'un programme de conformité

La démonstration de la conformité des traitements passe par la mise en place en interne d'une politique appropriée en matière de protection des données. Cette politique devra comprendre l'ensemble des principes nécessaires pour garantir la mise en œuvre de traitements équitables et transparents. Elle doit tenir compte des circonstances particulières et du contexte dans lesquels les données à caractère personnel sont traitées et elle organise les responsabilités opérationnelles.

L'identification des responsabilités des acteurs

Les organismes Hlm doivent s'attacher à identifier les responsabilités encourues en matière de traitement de données à caractère personnel en distinguant les cas de sous-traitance, des cas de responsabilité conjointe.

Les organismes Hlm ne doivent avoir recours qu'à des sous-traitants présentant des garanties suffisantes de mise en

œuvre de mesures techniques et organisationnelles appropriées pour garantir que leur traitement est conforme aux exigences du RGPD et protéger les droits des personnes concernées. Le contrat entre l'organisme Hlm et ses sous-traitants doit nécessairement être écrit.

Les mesures destinées à assurer la transparence sur les traitements

L'organisme Hlm doit disposer d'une politique de protection des données permettant de porter à la connaissance des personnes extérieures concernées par les traitements des informations prévues par la réglementation I&L et ce dans un format concis, transparent, compréhensible et aisément accessible.

Les mesures destinées à garantir les droits des personnes

L'organisme Hlm met en place une procédure facilitant l'exercice des droits des personnes (droit d'accès, de rectification, d'effacement, de limitation du traitement, à la portabilité. Cette procédure comprend, conformément à l'article 12 du RGPD, les modalités d'identification/authentification de la personne concernée exerçant ses droits, permettant de respecter les délais de réponse.

La procédure prévoit que le DPO pilote la gestion des demandes des personnes concernées relatives au traitement de leurs données et à l'exercice de leurs droits.

Les vérifications concernant la sécurité

En plus des éléments classiques relatifs à la sécurité du SI (disponibilité, intégrité, confidentialité, protection et résilience), ces vérifications peuvent ainsi porter sur :

- La pertinence des politiques de sécurité et leur respect par les personnels et sous-traitants.
- Le respect des normes /référentiels/ certifications applicables.

- Le suivi des préconisations de la filière SSI/DSI.
- Le respect des règles relatives aux durées de conservation, des demandes d'effacement et de limitation du traitement.
- L'existence de contrats écrits conformes aux exigences, ainsi que la mise en œuvre des garanties appropriées en cas de transferts de données à caractère personnel par le sous-traitant (comme la signature de clauses contractuelles types).
- La justification de la suppression des données traitées par le sous-traitant selon les termes contractuels.
- La sensibilisation et la formation des personnels.
- La réalisation par le sous-traitant d'audits et vérifications sur ses propres sous-traitants.
- La mise en place d'une procédure de notification d'une violation de données à caractère personnel à l'autorité de contrôle compétente, si possible dans les 72 heures après en avoir pris connaissance.

La réalisation des Analyses d'impact sur la protection des données (AIPD)*

L'AIPD a pour but de conduire à une analyse complète des risques par l'organisme Hlm. Elle est au cœur de la démarche de conformité prônée par le RGPD. Dans les cas, où elle n'est pas obligatoire, l'AIPD est un moyen d'assurer la conformité des traitements. Si elle révèle que malgré les mesures préventives prises, des risques résiduels importants demeurent, alors l'organisme Hlm doit saisir la CNIL pour consultation préalable.

Les organismes Hlm doivent être vigilants dans l'identification des traitements présentant des risques particuliers pour les personnes, qui n'étaient pas tous visés dans le « pack conformité logement social » et pour lesquels une AIPD devra être conduite, comme par exemple : la mise en œuvre de dispositifs reposant sur des objets connectés ou des capteurs (exemples : capteurs de prévention

des chutes pour les personnes âgées, capteurs se rapportant à la maîtrise de la consommation d'énergie...), pour lesquels il aura été au préalable déterminé que l'organisme Hlm avait la qualité de responsable de traitement.

La notification des violations de données*

Les organismes Hlm ont l'obligation de notifier à la CNIL les violations de données personnelles, lorsque la violation est susceptible d'engendrer un risque pour les droits et libertés des personnes concernées.

Les sous-traitants doivent par ailleurs notifier aux organismes Hlm toute violation de données dans les meilleurs délais après en avoir pris connaissance : cette obligation s'applique quel que soit le niveau de gravité.

Les personnes concernées disposent par ailleurs du droit d'être informées en cas de violation de leurs données personnelles, lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés.

L'audit des traitements

L'organisme Hlm doit formaliser une procédure d'audit de la conformité des traitements à la réglementation I&L.

Points de contrôle

C-15. Disposer d'une procédure de gouvernance des données personnelles au sein de l'organisme, permettant notamment d'identifier les responsabilités opérationnelles et de garder trace des avis / consultation du DPO.

C-16. Documenter les mesures correctives adoptées en cas de manquement constaté lors de l'examen de conformité aux AIPD et leur régulièrement mises à jour.

C-17. Assurer la formation de leur personnel, et notamment ceux ayant en charge la sécurité du système d'information, afin de leur permettre de conduire la démarche d'analyse des risques et de l'intégrer dans les processus opérationnels.

Outils et références

- Guide RGPD :
 - Livret 2 / Fiche n°17 : comment notifier les violations de données ?
 - Livret 2 / Fiche n°15 : comment conduire une AIPD ?
 - Référentiels thématiques de l'Union sociale pour l'habitat : Prise en compte et traitement des risques visés dans les référentiels USH
- RGPD : art. 36, 40 à 43
- G29/CEPD : Lignes directrices du 4 octobre 2017 [WP 248 rév.01]
- CNIL : Référentiel du label CNIL Gouvernance (ce label n'est plus délivré par la CNIL, mais son contenu reste pertinent)



BONNES PRATIQUES

ÉLÉMENTS DE LA POLITIQUE DE GOUVERNANCE DES ORGANISME HLM EN MATIÈRE DE PROTECTION DES DONNÉES PERSONNELLES

- Engagements de l'organisme Hlm concernant le respect des principes énoncés par le règlement européen général sur la protection des données responsabilités opérationnelles, y compris celles de la direction de l'organisme Hlm.
- Procédure de validation des traitements.
- Modalités de tenue du registre des activités de traitement.
- Modalités de conduite des analyses de risques et/ou d'impact sur la protection des données.
- Modalités d'encadrement du recours à la sous-traitance.
- Modalités de répartition des responsabilités en cas de responsabilité conjointe sur les traitements.
- Modalités de vérification que les mesures techniques, organisationnelles et de mise en conformité, en lien avec les analyses de risques et les AIPD, sont régulièrement testées, analysées et évaluées, afin de vérifier leur efficacité, notamment en cas de modification du risque présenté par le traitement.
- Rôles, missions et modalités d'intervention du DPO (exemple : Planning de réunions annuelles entre responsable de traitement et DPO, actions de sensibilisation à conduire, formalisation des recommandations, bilan annuel...). ●



BONNES PRATIQUES

CONTENU DE LA POLITIQUE DE PROTECTION DES DONNÉES À DESTINATION DES PERSONNES CONCERNÉES

La politique de protection des données de l'organisme Hlm doit comprendre :

- Toute information nécessaire pour garantir la mise en œuvre de traitements équitables et transparents, compte tenu des circonstances particulières et du contexte dans lequel les données à caractère personnel sont traitées.
- Les coordonnées de l'organisme Hlm, celles du délégué à la protection des données, ainsi que les engagements du demandeur concernant le respect des principes énoncés par le règlement européen général sur la protection des données, au regard notamment :
 - de la mise en œuvre de traitements licites ;
 - du respect des droits des personnes ;
 - des éventuels transferts vers un pays tiers ;
 - des destinataires des données collectées ;
 - de la durée de conservation des données collectées ;
 - des mesures de sécurité des données. •



BONNES PRATIQUES

ÉLÉMENTS DE LA PROCÉDURE D'AUDIT

La procédure d'audit permet d'apprécier :

- L'existence et l'efficacité de l'organisation et de la documentation pour gérer les traitements de données à caractère personnel dans le champ de l'audit.
- Les moyens alloués au DPO et l'efficacité de son action.

Elle permet de :

- Détecter les traitements mis en œuvre, et leur exhaustivité.
- Vérifier la conformité des traitements aux référentiels USH.
- Identifier les recours éventuels à des prestataires extérieurs.
- Caractériser la responsabilité des différents acteurs.
- Effectuer des contrôles pertinents sur les systèmes d'information par des auditeurs « techniques » afin de vérifier si les durées de conservation appliquées sont conformes aux durées prévues dans les référentiels USH, et que les données font l'objet d'une suppression effective à l'expiration de leur durée de conservation.
- Examiner la politique d'archivage des données à caractère personnel, le cas échéant, au regard des recommandations de la CNIL en la matière.
- Analyser et évaluer la démarche de sécurité.
- Vérifier l'identification des principaux risques que les traitements font peser sur les libertés et la vie privée des personnes concernées en cas d'atteinte à la sécurité des données à caractère personnel, en tenant compte des éventuels sous-traitants.
- Déterminer si les mesures de sécurité identifiées sont correctement mises en œuvre et s'appuient sur des vérifications adéquates effectuées sur les systèmes d'information, réalisées par des auditeurs « techniques ».
- Contrôler que les droits des personnes peuvent être exercés de manière effective, et dans des délais raisonnables. •

03

PARTIE LIVRET 1

Annexes

A. GLOSSAIRE

B. LISTE DES RÉFÉRENTIELS THÉMATIQUES USH DU LIVRET 3

**C. GROUPES DE TRAVAIL ET CONSULTATIONS EN VUE DE
L'ÉLABORATION DES RÉFÉRENTIELS USH**

ANNEXE A - Glossaire

Accountability ou Principe de responsabilité - (Article 5 du RGPD)

Obligation pour le responsable de traitement de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Analyse d'impact relative à la protection des données (AIPD)- (Article 35 du RGPD)

Méthode d'analyse de conformité et de risque permettant au responsable de traitement de démontrer la conformité des traitements. L'AIPD se décompose en trois parties :

- Une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels.
- L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité* concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques.
- L'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.

L'AIPD doit être menée avant la mise en œuvre du traitement. Elle doit être démarrée le plus en amont possible et sera mise à jour tout au long du cycle de vie du traitement.

Il est également nécessaire de revoir une AIPD de manière régulière pour s'assurer que le niveau de risque reste acceptable tout au long de la vie du traitement, dans la mesure où l'environnement, technique notamment, sera amené à évoluer, ce qui nécessitera d'adapter les mesures mises en œuvre.

Anonymisation (Considérant 26 du RGPD)

Les données sont considérées comme anonymes lorsque l'identification de la personne est impossible que ce soit par des moyens dont dispose le responsable de traitement ou un tiers. La réglementation I&L ne s'applique pas aux données « anonymisées ». Elle s'applique en revanche aux données pseudonymes.

Appréciations sur les difficultés sociales

Les appréciations sur les difficultés sociales (évaluation d'une situation sociale à partir d'un faisceau d'informations telles que des facteurs personnels et environnementaux) des personnes peuvent être rattachées aux catégories particulières de données dès lors qu'elles comportent des données sensibles ou peuvent permettre de déduire de telles informations. Le référentiel de l'Union sociale pour l'habitat n°2 autorise les traitements comportant des appréciations sur les difficultés sociales des personnes à des fins d'attribution, d'adaptation et de mutation des logements ou de la mise en œuvre d'un suivi social personnalisé.

Besoin d'en connaître

Le besoin d'en connaître est la nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée et pour la bonne exécution d'une mission précise. Ce principe implique notamment la mise en place de niveaux d'habilitation différenciés en fonction des besoins.

Certification/ Label en matière de protection des données - (Article 42 du RGPD)

Processus permettant l'obtention d'un label ou d'une certification délivrée par les organismes de certification. Tout comme l'adhésion à des codes de conduite, la certification est un des moyens permettant de démontrer la conformité des traitements.

Comité européen pour la protection des données (CEPD)

Vise le Comité institué par le RGPD et qui remplace l'ancien groupe de l'article 29 et a pour mission principale de veiller à l'application du RGPD dans tous les pays membres de l'UE.

Consentement (Article 4, 11° et 6, 1°(a) et 7 du RGPD), GR n°2 p29)

Le consentement joue un rôle central dans le RGPD. Il constitue l'un des fondements possibles pour traiter des données à caractère personnel, applicable notamment lorsqu'aucun autre fondement n'est envisageable (comme lorsque le traitement ne répond pas strictement à une mission d'intérêt public ou à une obligation légale). Lorsqu'il ne sert pas de fondement au traitement, il constitue une protection supplémentaire pour les personnes concernées en cas de collecte de données particulières. Le RGPD fixe les conditions de validité du recueil du consentement et prévoit le droit pour chaque personne de retirer son consentement.

Destinataire (Article 4, 9°) du RGPD)

« La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement ».

Données à caractère personnel (Article 4, 1°) du RGPD)

« Toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un

nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Données agrégées

Les données agrégées sont le résultat de fonctions permettant l'association de données et dont le but est de grouper un lot de données en vue d'obtenir un résultat synthétique. L'agrégation des données est le plus souvent nécessaire pour aboutir à l'anonymisation des données.

Données « sensibles » ou « particulières » (Article 9 RGPD)

Le RGPD relatif à la protection des données abandonne la notion de données « sensibles » au profit de celle de données « particulières ».

Il est interdit de collecter et traiter de manière informatisée des données particulières (santé, origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, données génétiques, les données biométriques, les données relatives à la vie sexuelle), sans le consentement exprès préalable des personnes concernées.

Données relatives à la santé (Article 4, 15° du RGPD)

Le RGPD comporte une définition extensive de la notion de données se rapportant à la santé qui inclue non seulement la santé physique, mais également les données relatives à la santé mentale ainsi que celles issues de la fourniture de prestation de santé dès lors qu'elles révèlent des informations sur l'état de la santé.

Fichier (Article 4, 6°) du RGPD)

« Tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

Finalité

La finalité du traitement est l'objectif principal de l'utilisation de données à caractère personnel. Les données sont collectées pour un but bien déterminé et légitime

et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.

Limitation du traitement (Articles 4, 3°, 18 et 23 du RGPD)

La limitation du traitement consiste « au marquage des données personnelles conservées en vue de limiter leur traitement futur », il peut s'agir du déplacement temporaire des données sélectionnées vers un autre système de traitement, ou dans le retrait temporaire des données publiées d'un site internet.

Loi Informatique et libertés ou loi I&L

Vise la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, telle que modifiée notamment en 2018 pour assurer la mise en cohérence de l'ensemble de la législation applicable à la protection des données à la suite de l'entrée en vigueur du RGPD le 25 mai 2018.

Minimisation (Considérant 39 et Articles 5, 19(c) du RGPD)

Le principe de minimisation des données impose au responsable de traitement que les données à caractère personnel soient adéquates, pertinentes et proportionnées, c'est-à-dire, limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées.

Points de contrôle

Les points de contrôles sont, dans une démarche de conformité, les éléments devant faire l'objet de vérification, selon une régularité à déterminer, afin d'assurer la conformité permanente d'un traitement. Ils sont définis par l'organisme Hlm au moyen de procédures et règles internes. Le présent Guide RGPD présente certains points de contrôles spécifiques pour assurer la conformité des traitements de données à caractère personnel avec la réglementation I&L.

Protection des données dès la conception (privacy by design) et protection des données par défaut (privacy by default) (Article 25 du RGPD)

La protection des données dès la conception concerne la mise en place d'une protection dès la création du système d'information ou du traitement, et ce, tout le long de ces traitements (par exemple :

la purge obligatoire du système, ou l'impossibilité de mémorisation des données bancaires plus de 2 heures). Tandis que la protection des données par défaut, vise le paramétrage applicatif, (exemple : permettre sur le profil de réseau social d'être paramétré pour ne pas être partagé).

Profilage (Articles 4,4° et 22 du RGPD et GR n°2 91)

Méthode permettant d'établir le profil d'une personne tant à des fins commerciales (segmentation comportementale) que dans le cadre de scores ou de cotation des risques.

Dans le cas où le profilage est utilisé pour prendre des décisions à l'encontre des intéressés, sa mise en œuvre est soumise à des conditions spécifiques (AIPD, consultations préalables). Les personnes concernées peuvent par ailleurs, s'opposer au profilage à des fins commerciales.

Proportionnalité - Voir « Minimisation »

Pseudonymisation (Article 4,5° du RGPD et GR n°2 p41)

Les données sont considérées comme pseudonymes lorsqu'elles ne peuvent plus être attribuées à une personne concernée sans avoir recours à des informations supplémentaires, pour autant que celles-ci soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir cette non-attribution à une personne identifiée ou identifiable.

Registre des activités de traitement (Article 30 du RGPD)

Le registre comporte la liste des traitements automatisés mis en œuvre au sein de l'organisme Hlm. Il doit être tenu à jour et peut prendre une forme papier ou électronique. Le registre répond à la nécessité d'assurer la transparence des traitements vis-à-vis des personnes concernées et de la CNIL.

Règlementation I&L

Vise le RGPD, la Loi Informatique et libertés et l'interprétation de ces textes par la CNIL et le CEPD et les juridictions.

Responsable de traitement (Article 4, 7°) du RGPD)

C'est la personne physique ou morale, l'autorité publique, le service ou l'organisme « maître du fichier », qui détermine les finalités et les moyens du traitement de données à caractère personnel.

Responsables conjoints du traitement (Article 26 du RGPD)

Le RGPD met en avant la notion de responsabilité conjointe lorsque deux ou plusieurs responsables de traitement déterminent conjointement les finalités et les moyens du traitement. Dans ce cas ils doivent définir leurs obligations respectives aux fins d'assurer le respect des exigences du RGPD, par voie d'accord entre eux, et en informer les personnes concernées. Cette exigence ne s'applique pas lorsque leurs obligations respectives sont définies par la loi.

Tiers autorisé

Voir "Destinataire" page précédente.

Traitement de données à caractère personnel (Article 4, 2°) du RGPD)

« Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

Traitement de « grande ampleur » ou « à grande échelle » (G29, WP 248, lignes directrices relatives à la conduite d'une AIPD)

La notion de traitement de « grande ampleur » renvoie soit au nombre de personnes concernées, en numéraire ou au regard de la population totale considérée, au volume des données traitées ou à leur variété, à la durée ou au caractère permanent du traitement.

Traitement « systématique » (G29, WP 248, lignes directrices relatives à la conduite d'une AIPD)

La notion de traitement de « systématique » renvoie aux cas suivants :

- Traitement réalisé en application d'un système ;
- Traitement prédéfini, organisé ou méthodique ; traitement réalisé en tant qu'élément d'une stratégie.

Violation de données à caractère personnel (Articles 4, 12° et 33 du RGPD et GR n°2 p84)

Le RGPD définit la violation de données à caractère personnel comme une « violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière ». Cette notion doit être entendue de manière plus large que celle de « faille de sécurité ». Elle est en effet définie par référence au contenu de l'obligation de sécurité (GR n°1).

ANNEXE B - Liste des fiches pratiques du Livret 2

FICHE N°1

Quelles sont les personnes pouvant avoir accès aux données traitées par l'organisme Hlm ?

FICHE N°2

Quelles sont les règles applicables à l'utilisation des champs libres et zones de commentaires ?

FICHE N°3

Quelles sont les règles à appliquer au traitement d'appréciations sur les difficultés sociales des personnes par les organismes Hlm ?

FICHE N°4

Dans quels cas et sous quelles conditions un organisme Hlm peut-il traiter de données relatives à la santé des résidents ?

FICHE N°5

Dans quels cas et sous quelles conditions un organisme Hlm peut-il traiter des données relatives aux infractions, condamnations pénales et mesures de sûreté ?

FICHE N°6

Quelles précautions en cas de traitement des données à caractère personnel relatives aux enfants ?

FICHE N°7

Comment assurer, en pratique, la transparence sur les traitements vis-à-vis des personnes concernées ?

FICHE N°8

Comment organiser et gérer la sécurité des traitements ?

FICHE N°9

Comment définir le cycle de vie des données ?

FICHE N°10

Quel est le cadre applicable au traitement du NIR par les organismes Hlm ?

FICHE N°11

Comment assurer la réalisation d'enquêtes en conformité avec le RGPD ? : enquêtes obligatoires et facultatives

FICHE N°12

Comment encadrer la vidéosurveillance ?

FICHE N°13

Quelles sont les précautions à prendre en cas de recours à des solutions d'habitat connecté ?

FICHE N°14

Comment tenir le registre et la documentation destinée à démontrer la conformité des traitements ?

FICHE N°15

Comment conduire des analyses d'impact relative à la protection des données (AIPD) ?

FICHE N°16

Comment recueillir le consentement et assurer sa traçabilité ?

FICHE N°17

Comment notifier les violations de données personnelles ?

ANNEXE C - Liste des référentiels thématiques de l'Union sociale pour l'habitat

REF USH N°1

Référentiel concernant le traitement de données à caractère personnel visant à enregistrer et instruire les demandes de logement social que ce soit en location ou en accession.

REF USH N°2

Référentiel concernant la gestion locative et patrimoniale du parc immobilier à caractère social et de ses accessoires.

REF USH N°3

Référentiel concernant la mise 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.

REF USH N°4

Référentiel concernant la gestion et suivi des incidents et du contentieux, permettant également de traiter des décisions de justice lorsqu'elles ont une incidence sur un lieu de résidence.

REF USH N°5

Référentiel concernant la mise en œuvre de dispositifs de vidéoprotection et de vidéo-surveillance.

REF USH N°6

Référentiel concernant la mise en œuvre de dispositifs de contrôle d'accès nominatifs aux locaux soumis à restriction d'accès.

ANNEXE D – Groupes de travail et consultations en vue de l'élaboration des référentiels de l'Union sociale pour l'habitat

Membres du Comité de pilotage

Représentants de la Direction des Politiques urbaines et sociales, de la Direction Juridique, de la Direction du Numérique et des Systèmes d'information, du DPO de l'Union sociale pour l'habitat, des représentants des fédérations Hlm (OPH, ESH, Coopératives) et des consultants associés à la démarche.

Membres des groupes de travail (DPO et responsables métiers)

Groupe de travail « Gestion de la demande »

- Habitats de Haute-Alsace
- Anaxia conseil (Habitats de Haute-Alsace)
- Groupe 3F
- SPTA
- CREHA ouest / SPTA
- Paris Habitat
- Groupe Arcade
- Clésence
- Sarthe Habitat
- DPMS (harmonie habitat, FDI)
- AREAL (SPTA)
- Domaxis (futur Seqens)
- Seqens
- France Habitation

Groupe de travail « Gestion locative et gestion du patrimoine immobilier »

- Habitats de Haute-Alsace
- Anaxia conseil (Habitats de Haute-Alsace)
- Paris Habitat
- Nantes Métropole Habitat

- Groupe Arcade
- OPAC 73
- Clésence
- Sarthe Habitat
- OPAC 38
- DPMS (Harmonie habitat, FDI)
- France Habitation
- Orne Habitat

Groupe de travail « Gestion des difficultés sociales et du contentieux »

- Habitats de Haute-Alsace
- Anaxia conseil (Habitats de Haute-Alsace)
- Batigère
- Paris Habitat
- Vilogia
- Nantes Métropole Habitat
- Groupe Arcade
- OPAC 73
- Clésence
- Domanys
- Sarthe Habitat
- DPMS (harmonie habitat, FDI)
- Seqens
- Harmonie habitat
- I3F

Groupe de travail « Référentiels sécurité et AIPD »

- Habitats de Haute-Alsace
- Anaxia conseil (Habitats de Haute-Alsace)
- Paris Habitat
- Valophis
- Batigère
- Vilogia
- Nantes Métropole Habitat
- Groupe Arcade
- OPAC 73
- Clésence
- Sarthe Habitat
- DPMS (Harmonie habitat, FDI)
- Domaxis (futur Seqens)
- France Habitation
- Harmonie habitat
- Dynacité
- 1001 vies habitat

Autres consultations

Directeurs des systèmes d'informations d'organismes, des représentants des clubs utilisateurs des progiciels de gestion utilisés par les organismes, des représentants du club Habsis.

LA COLLECTION DES CAHIERS, TOUTE L'EXPERTISE DE L'UNION SOCIALE POUR L'HABITAT

DERNIÈRES
PARUTIONS

COLLECTION REPÈRES

N° 94 - MAÎTRISE D'OUVRAGE, AMÉNAGEMENT ET URBANISME

Les Assises du foncier : Propositions sur l'accès au foncier pour la production de logements abordables (avril 2022)

N° 95 - MAÎTRISE D'OUVRAGE, AMÉNAGEMENT ET URBANISME

Comment initier une démarche de réemploi des matériaux ? (avril 2022)

N° 96 - MAÎTRISE D'OUVRAGE, AMÉNAGEMENT ET URBANISME

Comment gérer au mieux l'eau dans le bâtiment et le logement dès la phase de conception ? (mai 2022)

N° 97 - MAÎTRISE D'OUVRAGE, AMÉNAGEMENT ET URBANISME

Construire et réhabiliter les logements sociaux en intégrant le végétal (mai 2022)

N° 98 - HABITANTS/LOCATAIRES

Laïcité et vivre-ensemble : repères pour les organismes Hlm (mai 2022)

N° 99 - HABITANTS/LOCATAIRES

La cohabitation intergénérationnelle solidaire dans le logement social (juin 2022)

N° 100 - ÉNERGIE ET ENVIRONNEMENT

Le déploiement d'infrastructures de recharge de véhicules électriques au sein du parc Hlm (juin 2022)

N° 101 - DROIT ET FISCALITÉ

La taxe foncière sur les propriétés bâties et logements locatifs sociaux (juillet 2022)

N° 102 - FINANCEMENT

Les Hlm en chiffres, édition 2022 (août 2022)

N° 103 - MAÎTRISE D'OUVRAGE, AMÉNAGEMENT ET URBANISME

Transformation de l'existant et construction réversible (août 2022)

N° 104 - POLITIQUES SOCIALES

Construire sa raison d'être : enjeux et bénéfices d'une démarche transformante (septembre 2022)

COLLECTION PANORAMAS

N° 07 - ÉDITION 2020

Un panorama de recherches en cours dans le domaine de l'habitat et du logement

N° 08 - ÉDITION 2021

Un panorama de recherches en cours dans le domaine de l'habitat et du logement

N° 09 - ÉDITION 2022

Un panorama de recherches en cours dans le domaine de l'habitat et du logement

N° 10 - ÉDITION 2023

Un panorama de recherches en cours dans le domaine de l'habitat et du logement

N° 11 - POLITIQUES SOCIALES

Réalisations candidates au concours « Hlm, partenaires des âgés » 2021

COLLECTION ACTES

N° 24

Quoi de neuf acteurs ? La journée d'actualité du Réseau des acteurs de l'habitat (Journée d'étude du 20 mars 2019)

N° 25

Quoi de neuf chercheurs ? La vente de logements sociaux à l'épreuve de la recherche (Journée d'étude du 28 novembre 2019)

N° 26

Quoi de neuf acteur(s) ? Les Webinaires d'actualité du Réseau des acteurs de l'habitat (18 novembre et 8 décembre 2020)

N° 27

Réinventer la communication institutionnelle : le rapport d'activités à l'heure des vidéos et podcasts (Webinaires du 8 avril 2021)

N° 28

Être voisin(s). Espaces résidentiels et liens sociaux, aujourd'hui (Paris, 27 et 28 octobre 2021)

N° 29

Quoi de neuf, chercheurs ? Les défis d'un foncier et d'un logement abordables (Paris, 1^{er} décembre 2021)

N° 30

Faire avec les habitants : des collaborations renouvelées dans l'habitat social (Paris, 2 juin 2022)

Pour commander des Cahiers, se rendre sur l'espace « BOUTIQUE »
du site www.union-habitat.org

L'ensemble des Cahiers est disponible en PDF sur <http://ressourceshlm.union-habitat.org>,
après identification de l'utilisateur.

N°

105



**UNION NATIONALE
DES FÉDÉRATIONS D'ORGANISMES HLM**

14, rue Lord-Byron - 75384 Paris Cedex 08

☎ 01 40 75 78 00 - www.union-habitat.org