n°41

Repères

QUALITÉ DE SERVICE

Règlement européen relatif à la protection des données : impacts pour les organismes Hlm

Collection Cahiers - octobre 2017 - 25 €

L'UNION SOCIALE POUR L'HABITAT
Les Hlm, habiter mieux, bien vivre ensemble

Publication de l'Union sociale pour l'habitat

PILOTAGE ET COORDINATION

Magali Vallet, conseillère en politiques sociales, Direction des politiques urbaines et sociales et correspondante informatique et libertés de l'Union sociale pour l'habitat, **Antoine Ferré,** directeur de la mission numérique Hlm, **Juliette Furet**, responsable du département des politiques sociales, Direction des politiques urbaines et sociales.

RÉALISATION

Maître Nathalie Metallinos, Idea AARPI.

CONTRIBUTIONS DES CORRESPONDANTS INFORMATIQUE ET LIBERTÉS ET EXPERTS

› **Afif Benyahya,** Lille Métropole Habitat - **Christophe Champoussin,** Anaxia Conseil - **Véronique Chatonnier,** Paris Habitat - **Frank Claes,** ICF Habitat - **Fabienne Desruelle,** I3F - **Malika El Abed,** Nantes Métropole Habitat - **Nathalie Lemaire et Jessika Noel,** Nièvre Habitat - **Vanessa Lesigne et Micheline Suchod,** Habitat en Région - **Rebiha Ouari,** Domaxis - **Elisabeth Pinto,** Fédération des ESH - **Laetitia Reina,** Opac 38 - **Jean-Yves Thomas,** Groupe Batigère - **Marc Zumbrunnen,** Groupe Valophis.

Maquette et réalisation : 62Avenue, Paris - Impression : DEJALINK - Stains - octobre 2017.

Photo couverture : ©Shutterstock

sommaire

Références utiles

Dans un contexte de développement des outils du numérique et du digitale, d'accroissement des flux de données à l'intérieur même des organismes Hlm mais aussi vers l'extérieur, la protection des données à caractère personnel constitue un enjeu majeur.

En 2014, la publication du pack de conformité « logement social » a provoqué une véritable prise de conscience de la nécessité de progresser dans l'application des dispositions de la loi informatique et libertés. Trois ans après, on observe que la plupart des organismes se sont appropriés le pack et ont mis en œuvre une démarche de mise en conformité. Certains ont recruté des correspondants informatique et libertés, d'autres ont mutualisé leurs moyens et externalisé la fonction.

Si des efforts restent à faire, le chemin parcouru est énorme.

Pour atteindre cet objectif, il a fallu convaincre les directions générales, seules à même d'impulser la démarche de mise en conformité. L'Ush s'est également fortement mobilisée en rédigeant un guide repère n°1 relatif à la mise en œuvre du pack de conformité « logement social » à destination de l'ensemble de ses adhérents, et en réalisant un tour des régions pour expliciter et sensibiliser sur la nécessité de se mettre en ordre de marche.

Le 27 avril 2016, le règlement européen relatif à la protection des données à caractère personnel et à la libre circulation des données était adopté par le Parlement européen. Ce règlement européen intervient deux ans après la publication du pack de conformité « logement social ». Publié au JO de l'Union Européenne le 4 mai 2016, le RGPD est entré en vigueur le 24 mai 2016. Après une période transitoire de 2 ans pour se mettre en conformité, il entrera en application le 25 mai 2018. Ses dispositions s'appliqueront à l'ensemble des organismes Hlm, comme à l'ensemble des entreprises.

Si on y retrouve les principes essentiels de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le règlement (RGPD) instaure de nouvelles dispositions et un changement total de paradigme via la disparition progressive des formalités déclaratives au profit du concept de mise en responsabilité (« accountability »).

Editorial

Parmi les principales mesures figurent :

- Le principe de responsabilité (« accountability ») et la prise en compte de la protection des données dans dès la conception de tout nouvel applicatif ou à l'occasion de tout nouveau traitement de données (« privacy by design »).

- La transformation du correspondant Informatique et libertés (CIL) en délégué à la protection des données (data protection officer - DPO).

- La mise en place d'études d'impacts pour les traitements comportant des données sensibles.

- Il renforce également le droit des personnes, les responsabilités des sous-traitants et relève le niveau des sanctions.

La présente publication s'inscrit dans le prolongement du guide Repères n°1, avec pour vocation d'accompagner les organismes dans tous ces changements, ces évolutions. Elle propose une présentation des principaux concepts du RGPD et détaille ensuite l'ensemble des mesures du RGPD, impactant les organismes.
En parallèle, les outils opérationnels destinés à outiller les organismes et disponibles sur le site internet de l'Union sociale pour l'habitat, dans sa rubrique « *espace collaboratif : réseau informatique et libertés* » ont été mis à jour.

Le mouvement professionnel a une responsabilité vis-à-vis des locataires qui confient en toute confiance leurs données. Aussi, les organismes doivent poursuivre leurs efforts de mise en conformité. Ce guide est un outil mais il devra s'accompagner d'une implication très forte des directions générales afin de sensibiliser l'ensemble des collaborateurs.

Jean-Louis Dumont,
Président de l'Union sociale pour l'habitat

PARTIE 1

Un nouveau guide sur la protection des données personnelles : pourquoi faire ? pour qui ?

DE NOUVELLES RÈGLES D'APPLICATIONS À COMPTER DU 25 MAI 2018

Le RGPD impose des mesures de protection des données traitées aux entreprises multinationales, qui seront soumises aux même règles et sanctions que les entreprises européennes. Il permet d'assurer ainsi une continuité de la protection des données, même en cas de franchissement de frontières.

L'adoption le 27 avril 2016 d'un nouveau règlement européen sur la protection des données (RGPD), en tant que **cadre de référence commun en matière de protection des données à caractère personnel,** est l'aboutissement de quatre années de discussions intenses sur l'orientation et les moyens propres à assurer **la protection des libertés publiques** face aux défis posés par **les évolutions technologiques** et la diffusion accrue des données personnelles compte tenu des flux internationaux de données.

Une continuité des principes, mais une nouvelle méthodologie

Le nouveau cadre posé par le RGPD, qui est **d'application directe à compter du 25 mai 2018**, s'inscrit dans **la continuité des règles et principes déjà en place en France** depuis 1978, et au niveau européen depuis 1995, retranscrites dans la Loi Informatique et libertés modifiée en 2004 et 2016. Les règles et principes applicables au traitement de données à caractère personnel ont été normés et explicités pour les organismes Hlm, dans le « **Pack de conformité logement social** » adopté par la CNIL en 2014, à la suite d'une large concertation avec les organismes Hlm. La publication du **Repères n°1** « *Mise en œuvre du pack de conformité logement social de la CNIL* » a permis d'apporter aux organismes Hlm des recommandations pratiques et de proposer **une démarche de conformité,** visant à assurer l'effectivité des règles de protection des données à caractère personnel.

Le RGPD nécessite d'adapter les processus engagés par les organismes en 2014. Il instaure une méthodologie qui est, en partie, nouvelle. Ainsi, ce qui n'était que recommandation dans la Loi Informatique et libertés, devient une obligation à compter du 25 mai 2018 et les organismes Hlm sont invités à confronter leur démarche avec la nouvelle méthodologie prônée par le RGPD qui présente les caractéristiques suivantes :

- Elle est plus exigeante que celle initialement préconisée pour assurer le respect de la Loi Informatique et libertés.
- Elle intègre une approche « par les risques » permettant aux organismes Hlm d'adapter le niveau d'exigence aux risques encourus par les personnes concernées du fait du traitement de leurs données à caractère personnel, ainsi qu'à la taille, les moyens et la structure de l'organisme Hlm.
- Elle nécessite des connaissances approfondies, tant sur le droit de la protection des données à caractère personnel, que sur la sécurité informatique, ainsi que la démarche d'audit, de conformité et d'évaluation des risques.

› Elle place le délégué à la protection des données (qui remplace le CIL) au cœur de la démarche.

› Elle impose une formalisation accrue des analyses (de conformité réglementaire et de risques pour les personnes concernées par les traitements de données à caractère personnel), ainsi que la réalisation régulière de vérifications et audits sur les traitements et les sous-traitants permettant de démontrer la conformité.

› Elle demande enfin que les organismes Hlm identifient les rôles et responsabilités sur les traitements de données à caractère personnel et mettent en place une organisation appropriée (procédures, circuits de validation, règles de gouvernance, désignation d'un délégué à la protection des données…) destinée à assurer l'effectivité de la protection des données à caractère personnel et de la vie privée.

› Enfin, le RGPD porte le montant des sanctions encourues à 20 millions d'euros ou 4% du chiffre d'affaires mondial consolidé.

Des enjeux renforcés pour les organismes Hlm

Tout comme pour la mise en œuvre du « Pack de conformité logement social », la prise en compte des exigences du RGPD permet :

› d'assurer la sécurité juridique de la conduite des activités des organisme Hlm, en protégeant les organismes Hlm contre respectivement les sanctions administratives de la CNIL (injonction de cesser les opérations de traitement, demande de destruction des données, sanction financière), ainsi que les sanctions pénales,

› de conforter et d'assurer la concrétisation de l'engagement éthique et citoyen des organismes Hlm, en préservant la vie privée des locataires et employés et en assurant la sécurité de leurs données à caractère personnel,

› de renforcer la qualité de service, en assurant la qualité des données traitées et la sécurité des systèmes d'information, ce qui est particulièrement important compte tenu de l'augmentation des attaques de cybercriminels et des failles de sécurité.

Elle constitue **une étape supplémentaire et indispensable** pour assurer la conformité des traitements de données à caractère personnel mis en œuvre par les organismes Hlm, et tout particulièrement, ceux mis en œuvre au titre de leurs missions de service public qui entraînent le traitement de données sensibles des demandeurs et bénéficiaires de logements sociaux.

La poursuite des démarches engagés de mise en conformité

La mise en œuvre du RGPD au sein des organismes Hlm nécessite **un effort important** de poursuite et d'adaptation du chantier entrepris depuis 2014, voire antérieurement pour les organismes les plus avancés. **Les directions générales jouent un rôle-clé dans le déploiement du RGPD :**

› d'une part, il place sur elles la responsabilité de la conformité des traitements, et donc de l'organisation interne permettant de l'assurer. Toutes les fonctions, opérationnelles et supports, sont impactés, le sujet de la protection des données étant transverse ;

9. La base SISAL prend en compte le coût complet des opérations, charges foncières incluses

› d'autre part, la mise en œuvre de la réforme impacte tout autant l'aspect stratégique de la conduite des opérations (*décider de mettre en œuvre tel traitement sous telles conditions*) que la conduite courante des opérations qui vont devoir intégrer les nouvelles règles. Il en va de même pour l'adaptation des systèmes d'informations qui doit se poursuivre pour intégrer, comme le RGPD l'exige désormais, la protection des données à caractère personnel **dès la conception des systèmes et applications informatiques**, ainsi que dans le paramétrage de ces dernières.

L'accompagnement des organismes par l'Union sociale pour l'habitat

La mise en œuvre du plan d'accompagnement opérationnel dès 2014 place les organisme Hlm dans une position plus favorable que les acteurs d'autres secteurs d'activité qui « découvrent » le sujet. L'objectif est désormais de tirer profit de cette avance pour consolider les acquis et intégrer, dans les délais, les nouveautés.

Ce guide présente les modifications essentielles apportées par le règlement général sur la protection des données en mettant l'accent sur les modifications impactant les organismes Hlm.

› Il vise, tout comme le Cahier **Repères n°1**, à identifier les actions prioritaires à mettre en œuvre par les organismes Hlm.

› Il incorpore les recommandations et lignes directrices d'ores et déjà adoptées par les autorités de la protection des données (CNIL et G29[1]).

› Il comporte des fiches pratiques et des recommandations opérationnelles, et actualise le plan d'actions du Cahier **Repères n°1**.

À RETENIR

L'actualisation de ces informations sera assurée notamment par la veille postée sur l'espace collaboratif « informatique et libertés » du site internet de l'Union sociale pour l'habitat, au fur et à mesure de l'adoption de recommandations, de modifications législatives et des apports jurisprudentiels.

[1] Groupe Article 29

PARTIE 2

Le nouveau cadre européen fixé par le RGPD relatif à la protection des données à caractère personnel

LE NOUVEAU CADRE EUROPÉEN

Le cadre européen de la protection des données est régi depuis 1995 par la Directive 95/46/CE du 24 octobre 1995[2] (directive générale sur la protection des données) qui constituait – jusqu'à l'adoption du Règlement général relatif à la protection des données le 27 avril 2016[3] – le texte de référence, au niveau européen, en matière de protection des données à caractère personnel.

Présentation générale

La Directive 95/46 fixait des limites strictes à la collecte et à l'utilisation des données à caractère personnel, et posait notamment les principes relatifs à la légitimation et à la licéité des traitements de données à caractère personnel et à la qualité de ces données. La Directive 95/46 a été transposée en droit français par la loi du 6 août 2004 qui a notamment introduit la fonction du CIL.

Même si les principes de protection des données et droits des personnes sont dans leur essence reconduits, assurant ainsi **la continuité dans la régulation**, son adoption marque **un changement de méthode** avec une place accrue à **l'autorégulation** et à un **accroissement de la responsabilité des organismes** traitant des données à caractère personnel (responsables de traitements, sous-traitants) qu'ils soient situés ou non dans l'Union européenne.

Son adoption vise à adapter **la législation aux nouveaux défis du numérique** et à créer **un niveau élevé et uniforme de protection des données à travers l'Union européenne** à la hauteur des enjeux pour les droits et libertés, et tenant pleinement compte de la place des technologies de l'information et des communications (téléphones intelligents, médias sociaux, services bancaires sur Internet, transferts internationaux, informatique en nuage et internet des objets...) et des dangers qu'un développement incontrôlé fait peser sur les droits et libertés des citoyens.

À NOTER

Le règlement renforce les droits des citoyens européens notamment en leur donnant plus de contrôle sur leurs données personnelles :

- par **de nouveaux droits** (droit à l'oubli numérique, droit à l'effacement, droit à la portabilité) et par l'introduction d'un principe de responsabilité (« accountability »),
- par **un renforcement des règles de transparence imposées aux responsables de traitements** afin d'assurer la loyauté de la collecte et de nouveaux droits (droit à l'oubli numérique, droit à l'effacement, droit à la portabilité, droit à l'oubli – quasi-automatique – sur Internet pour les mineurs),
- il rend ainsi plus exigeante l'application de la législation en matière de protection des données personnelles.

2. Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
3. Règlement (UE)n° 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données

De nouvelles règles pour les citoyens, les responsables de traitements de données personnelles, les autorités de protection

De nouveaux droits pour les citoyens

› **Le droit à l'oubli est revisité :** il comporte désormais des déclinaisons nouvelles (droit à l'effacement, droit au déréférencement, droit à la limitation du traitement).

› **La place du consentement est renforcée :** la personne concernée est mieux à même de contrôler l'utilisation de ses données personnelles.

› **Une plus grande transparence sur les traitements est exigée :** les personnes concernées disposeront d'une information préalable plus complète et accessible.

› **Le droit de transférer ses données** vers un autre fournisseur de services (portabilité).

› **Le droit pour les personnes concernées d'être informées en cas de piratage** ou de perte des données (notification des violations de données).

› **La garantie que les données seront protégées** par la mise en œuvre de la protection dès la conception et par défaut.

Les changements pour les responsables de traitements

› **L'allègement des formalités** et la mise à disposition d'outils de conformité (registre, délégué à la protection des données, étude d'impact sur la vie privée, codes de conduite/certifications ...) qui pourront être modulés en fonction du risque sur les droits et libertés des personnes.

› **Une mise en œuvre plus stricte des règles et principes** (l'obligation de documenter l'ensemble des traitements et de pouvoir rendre compte de leur conformité), y compris en cas de flux transfrontaliers.

› Pour les entreprises multinationales, **la possibilité d'un interlocuteur unique** (guichet unique) pour toutes les autorités de protection des données européennes.

› **La création de nouvelles règles d'application extraterritoriale** aux opérations de traitement réalisées hors du territoire de l'Union européenne liées à une offre de biens ou de services en direction de personnes physiques situées sur le territoire de l'Union européenne (y compris à titre gratuit), ou ayant pour objet le suivi du comportement de ces personnes au sein de l'Union européenne.

Des pouvoirs renforcés pour les autorités de protection des données personnelles (la CNIL en France)

› Une affirmation de leurs compétences (extraterritorialité) dès lors qu'il existe un établissement sur le territoire de l'Union ou que leurs citoyens sont affectés par le traitement.

› Le renforcement de leurs pouvoirs, notamment répressifs avec la possibilité de prononcer des sanctions administratives pouvant aller jusqu'à 4% du chiffre d'affaires mondial de l'entreprise concernée.

› Des règles de coopération et concertation au niveau européen permettant de tenir compte de la nature transfrontière des traitements de données à caractère personnel et d'éviter que les responsables de traitements profitent des disparités entre les droits des États membres pour choisir l'interprétation la plus favorable à leurs intérêts.

› La création d'un nouvel organe européen qui prend la suite du G29 mais qui est doté de pouvoirs plus importants dont celui de rendre des avis contraignants : **le Comité européen de la protection des données** (CEPD) en charge d'arbitrer les différends entre les autorités et également d'élaborer la « doctrine européenne ».

COMMENTAIRE

L'adoption du règlement européen sur la protection des données personnelles le 27 avril 2016, constitue l'aboutissement de quatre années de travail et de négociations intenses, et marque un tournant majeur dans la régulation des données personnelles.

Au vu de l'importance des changements introduits et des enjeux, son adoption marque **le début d'un compte à rebours** de deux ans, jusqu'à la mise en œuvre effective en mai 2018.

LES IMPACTS PRÉVISIBLES DE LA RÉFORME SUR LE DROIT NATIONAL

La loi pour une République numérique du 7 octobre 2016[4] a créé de nouveaux droits pour les personnes concernées et a renforcé considérablement les pouvoirs de sanctions de la CNIL qui voit ses missions renforcées. Certaines des dispositions anticipent l'application du règlement européen sur la protection des données personnelles.

Nouvelles règles de transparence

Les responsables de traitements doivent assurer l'information des personnes sur la durée de conservation de leurs données ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée (modification de l'article 32 de la Loi Informatique et libertés).

Création de nouveaux droits

- Le droit à l'oubli pour les mineurs pour les données collectées sur Internet : la loi créee un « droit à l'oubli » spécifique aux mineurs et prévoit une procédure accélérée pour l'exercice de ce droit. En l'absence de réponse ou en cas de réponse négative de la plateforme dans un délai d'un mois, la personne peut saisir la CNIL qui dispose alors d'un délai de trois semaines pour traiter la saisine.

- L'affirmation du droit à l'autodétermination informationnelle : ce droit renforce la capacité de l'individu à maîtriser les usages qui sont faits de ses données à caractère personnel.

- La possibilité d'exercer ses droits par voie électronique (nouvel article 43 bis de la loi Informatique et Libertés) impose, "lorsque cela est possible", de permettre à toute personne l'exercice des droits d'accès, de rectification ou d'opposition par voie électronique, si le responsable du traitement des données les a collectées de cette manière.

- Le droit à la portabilité sur des données autres que personnelles[5].

Le rôle de la CNIL dans l'accompagnement de l'ouverture des données publiques

- Toute mise à disposition ou réutilisation de données personnelles à d'autres fins que celles pour lesquelles elles ont été détenues est soumise à la Loi Informatique et libertés : la CNIL a ainsi annoncé l'élaboration d'un « pack de conformité » en matière d'ouverture des données publiques.

- La CNIL acquiert la possibilité d'homologuer des méthodologies d'anonymisation.

4. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
5. Cf. Fiche de synthèse n°5 pour l'impact en annexe

Utilisation du NIR pseudonymisé à des fins de recherche scientifique ou historique.

› Allègement des formalités pour les travaux statistiques et de recherche scientifique et historique via la création d'un « code spécifique non signifiant » obtenu au moyen d'une opération cryptographique du NIR, dont les modalités seront précisées par décret en Conseil d'État pris après avis de la CNIL.

Compétences de la CNIL renforcées

› Le plafond maximal des sanctions de la CNIL passe de 150 000 € à 3 millions. Ceci constitue une anticipation sur l'augmentation du plafond du montant des sanctions prévue par le règlement européen (plafond pouvant aller jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, 4% du chiffre d'affaires mondial à compter du 25 mai 2018).

› Possibilité pour la CNIL d'ordonner que les organismes sanctionnés informent individuellement des sanctions et à leur frais, chacune des personnes concernées, de prononcer des sanctions financières sans mise en demeure préalable des organismes lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité.

› Avis de la CNIL rendu obligatoire sur les projets de loi ou de décret relatifs à la protection des données à caractère personnel ou au traitement de telles données, est rendue obligatoire. La publicité sur les sanctions prononcées devient systématique.

Les nouvelles missions de la CNIL

› La promotion de l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données.

› La certification de la conformité des processus d'anonymisation des données personnelles dans la perspective de leur mise en ligne et de leur utilisation.

› La conduite par la CNIL d'une réflexion sur les problèmes éthiques et les questions de société soulevées par l'évolution des technologies numériques.

LES MODIFICATIONS ATTENDUES DE LA LOI INFORMATIQUE ET LIBERTES

Le Règlement général relatif à la protection des données entrera en application le 25 mai 2018, sans qu'il soit nécessaire pour les États membres d'adopter des actes de transposition. Les États gardent cependant la possibilité de légiférer en restant conformes au RGPD : la loi Informatique et libertés sera harmonisée avec les dispositions du règlement. Dans cette attente, le RGPD est le texte de référence.

Le RGPD contient de multiples possibilités pour les États membres de prévoir des dérogations ou des adaptations. C'est notamment le cas pour les traitements du secteur public (sécurité nationale, défense, police, justice, fiscalité, sécurité sociale, santé et autres intérêts publics importants), ainsi que ceux mis en œuvre à des fins d'emploi, de recherche historique et scientifique.
Le RGPD prévoit également des possibilités d'adaptation pour assurer la liberté d'expression, le respect des secrets protégés par la loi, l'accès aux documents administratifs, la gestion des identifiants nationaux (comme le NIR).

Le projet de modification de la Loi Informatique et libertés est en cours de rédaction. Il devrait intégrer les nouvelles mesures prévues par le RGPD et contenir des spécificités propres à la France.

En complément, des **actes délégués** seront adoptés par la Commission européenne **pour détailler l'application du règlement**. Aussi, contrairement à l'effet d'annonce, et plus particulièrement dans le secteur public, le RGPD ne va pas permettre une harmonisation totale : de nombreuses disparités et des régimes spécifiques, devraient demeurer dans les États membres.

À NOTER

Les organismes Hlm devront être particulièrement vigilants au maintien éventuel, dans la Loi Informatique et libertés modifiée à venir, de certains régimes spécifiques de formalités (des autorisations pourraient être nécessaires pour la modification de traitements visés au « Pack de conformité logement social »).

À RETENIR

Autres textes de référence

La Loi Informatique et libertés et demain le RGPD, doivent également s'articuler avec les dispositions du code des relations entre le public et l'administration (récemment modifiée par la loi pour une République numérique), la loi sur l'obligation, la coordination et le secret en matière statistique (loi du 7 juin 1951), ainsi que les dispositions du code du patrimoine relatives aux archives.

Le nouveau rôle de la CNIL

L'allègement des formalités conduit la CNIL à centrer son action sur la mise à disposition d'outils de conformité, ainsi que sur le contrôle de l'effectivité de l'application du RGPD.

Certification et adoption de référentiels

La CNIL acquiert avec le RGPD une nouvelle activité de certification ce qui va la conduire à poursuivre le travail déjà entamé avec les packs de conformité, avec l'adoption de nouveaux référentiels.

Pouvoir de contrôle et sanction réaffirmés

La CNIL va pouvoir adopter des sanctions dissuasives afin d'assurer l'effectivité de l'application du RGPD. Le montant des sanctions passe en effet de 3 à 20 millions € (ou 4% du chiffre d'affaire mondial consolidé).

Outils de conformité mis à disposition par la CNIL pour accompagner les responsables de traitements dans la mise en œuvre du RGPD[6]

- **Des fiches pratiques**
  - LE RGPD : une méthodologie en 6 étapes
  - La priorisation des risques (*Cf. guide sécurité de la CNIL*)
  - La documentation de la conformité

- **Des guides :** catalogue de bonnes pratiques pour aider à déterminer les mesures proportionnées aux risques identifiés
  - PIA-1, la méthode : Comment mener une étude d'impact sur la vie privée
  - PIA-2, l'outillage : Modèles et bases de connaissances de l'étude d'impact sur la vie privée
  - PIA-3, les bonnes pratiques : Mesures pour traiter les risques sur les libertés et la vie privée

- **De nouvelles procédures**
  - Formulaire de notification de violation de données personnelles
  - Formulaire de désignation du délégué à la protection des données

Cf. Fiche de synthèse n°1, page 86.

- Manquements majeurs : 20 M€ ou 4% du CA annuel mondial
- Autres manquements : 10 M€ ou 2% du CA annuel mondial
- **Du 7 octobre 2016 au 24 mai 2018 : 3 M€ (tout type de manquements)**

6. www.cnil.fr/fr/tag/R%C3%A8glement+europ%C3%A9en

PARTIE 3

Impact du RGPD pour les organismes Hlm : les fondamentaux

L'ESSENTIEL DES MODIFICATIONS

Les principes présidant à la collecte et au traitement de données à caractère personnel figurant dans la Loi Informatique et libertés (licéité et loyauté, finalité, proportionnalité, exactitude et mise à jour des données, durée de conservation limitée, sécurité : cf. Repères n°1) sont reconduits pour l'essentiel dans le RGPD. Toutefois, sous cette apparente continuité, le RGPD revoit en profondeur certaines règles affectant ainsi l'application des principes.

La grande nouveauté concerne **la suppression de la plupart des formalités** de déclaration au profit de l'introduction **du principe de responsabilité** (« *accountability* ») qui entraîne notamment pour les responsables de traitements **l'obligation de démontrer la conformité** des traitements à la législation en matière de protection des données personnelles (cette démonstration se fait notamment par l'adoption de mesures organisationnelles [procédures, formation des personnels..], la conduite de vérifications [audits], la tenue d'une documentation sur les traitements ...). En découle pour le responsable de traitement, **la mise en place de mesures visant la protection des données dès la conception de tout traitement comportant des données à caractère personnel** (« *privacy by design and by default* »), et tout au long de son développement. Il en résulte un contrôle plus exigeant des conditions de licéité autorisant le traitement des données à caractère personnel.

Le règlement impose aux responsables de traitement une efficacité accrue des mécanismes visant à garantir le respect des droits et libertés des personnes. Il durcit **les conditions applicables au recueil du consentement et renforce les exigences de transparence.** Par ailleurs, le RGPD prévoit le renforcement des **missions du correspondant informatique et libertés** (CIL), qui devient **le délégué à la protection des données** (DPO pour « Data Protection Officer »). Ses missions sont **confirmées** et concernent tous les traitements mis en œuvre par le responsable de traitement et comportant des données à caractère personnel (indépendamment des formalités à accomplir).

À NOTER

Les principes que doivent continuer à appliquer les organismes Hlm

› **Licéité, loyauté et transparence :** des données obtenues et traitées de manière licite, loyale et transparente.

› **Limitation des finalités :** des données collectées pour des finalités déterminées, explicites et légitimes et qui ne sont pas utilisées ultérieurement de manière incompatible avec ces finalités.

› **Minimisation des données :** des données adéquates, pertinentes et limitées[7] à ce qui est nécessaire au regard des finalités poursuivies.

› **Exactitude :** des données exactes et si nécessaire mises à jour.

› **Limitation de la conservation :** des données conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées (exceptions : archives publiques[8], recherche scientifique et historique).

› **Intégrité et confidentialité :** il s'agit de prendre toutes les mesures, d'ordre technique ou organisationnel, afin d'assurer la sécurité des données et de prévenir toute détérioration, perte ou destruction.

› **Mise en application du droit des personnes** (droit d'opposition, d'accès, de rectification, de limitation...).

7. La notion de « minimisation » introduite par le RGPD se substitue au principe de proportionnalité des traitements qui vise le recueil de données « non excessives au regard des finalités du traitement ». Les organismes Hlm devront ainsi, de manière encore plus rigoureuse, justifier du traitement de telle ou telle donnée au regard de la finalité du traitement.
8. « à des fins archivistiques dans l'intérêt public ».

	AVANT	APRÈS
Formalités	› Formalités déclaratives préalables à la mise en œuvre de tout traitement comportant des données à caractère personnel. › Exception pour les traitements relevant du régime de la déclaration normale et simplifiée, dès lors qu'un CIL est nommé.	› Disparition de la plupart des formalités déclaratives au profit du principe de responsabilité (« accountability »), qui se traduit par l'obligation de documenter la démarche de mise en conformité, et l'obligation de mettre en place toutes les mesures de sécurité nécessaires dès la mise en place de tout nouveau traitement (« privacy by design »)
Responsabilités	› Seul le responsable de traitement peut être mis en cause et sanctionné cas de défaillance (faille de sécurité, violation de données…)	› Création de la responsabilité conjointe lorsque plusieurs responsables de traitement interagissent sur un même traitement ; › Mise en place d'une responsabilité propre aux sous-traitants.
Droit des personnes renforcés	› Droit d'accès pour toute personne concernée par un traitement de donnée ; › Le responsable de traitement dispose de deux mois pour répondre aux demandes d'accès.	› De nouvelles informations doivent apparaître dans les mentions obligatoires ; › Renforcement des exigences en matière de recueil du consentement + modalités de retrait du consentement ; › Un mois pour répondre aux demandes d'accès + possibilité d'actionner le droit d'accès par voie électronique
CIL/DPO	› Nomination d'un CIL facultative ; › Le CIL peut être mutualisé et/ou externalisé ; › Le CIL tient un registre et dresse un bilan annuel de son activité.	› Le CIL devient DPO. Il n'est pas responsable en cas de défaillance. Seul le responsable de traitement peut être sanctionné. › le DPO a une mission d'audit et de contrôle renforcé, par rapport au CIL. › Le DPO devient obligatoire pour les bailleurs en raison de leur statut pour les OPH et du traitement à grande échelle pour l'ensemble des organismes Hlm, quel que soit leur statut. › Le DPO peut être mutualisé et/ou externalisé. › Le registre devient obligatoire du fait du traitement de données sensibles par les bailleurs sociaux.

TÉMOIGNAGE

Véronique Chatonnier, CIL de Paris Habitat*

La mise en place du RGPD

Le RGPD est un nouveau défi comme l'a été le déploiement du « Pack de conformité logement social ». C'est une très grande marche à franchir en termes de mise en place de documentation (rédaction de politiques et procédures intégrées aux processus métiers) dans une logique d'« *accountability* » .

Le RGPD a un effet structurant, il permet de conforter la démarche déjà entreprise par le « Pack de conformité logement social » et implique une plus grande réflexion concernant la gouvernance du patrimoine informationnel de l'organisme Hlm.

Premières actions et réalisations

- Traitement des points de conformité les plus sensibles : durées de conservation, zones de commentaires, habilitations informatiques, traçabilité... afin d'assurer le respect des principes de base de la protection des données.
- Mise en place de mentions d'information.
- Sensibilisation du personnel.
- Rédaction d'un livre blanc du métier de gardien en concertation avec la profession et les associations de locataires.
- Mise en place du registre et recensement des traitements.
- Mise en place d'un espace intranet.
- Vidéo de sensibilisation à destination de l'ensemble du personnel.
- Rédaction de notes thématiques et de référentiels métiers.
- Campagnes de tri et d'archivage des dossiers papier.
- Audit du SI fin 2015 et plan d'actions entrepris en 2016.

Préparer l'arrivée du RGPD

- Adaptation du plan d'actions défini en 2016.
- Présentation du RGPD au CODIR.
- Préparation d'un guide avec les implications du RGPD.
- Rédaction de politiques et procédures communes au RGPD et plan d'actions sécurité.
- Actualisation et extension du registre.

Conseils aux futurs DPO

- Valider la répartition des tâches entre le DPO et le RSSI/DSI
- Redéfinir le plan d'actions au regard de la future réglementation.
- Intégrer le RGPD dans les processus métiers et lier toute la politique de sécurité du DSI au RGPD.

* OPH, 130 000 logements, 2 953 collaborateurs

LA DISPARITION DES FORMALITES AU PROFIT D'UNE DEMARCHE DE RESPONSABILITE (« ACCOUNTABILITY »).

Le règlement général relatif à la protection des données met fin au régime de droit commun de déclaration tel que contenu dans la Loi Informatique et libertés.* Cette suppression est une conséquence du principe de responsabilité (« accountability »).

Principe

L' « *accountability* » englobe non seulement la notion de **responsabilité** mais impose également une obligation **d'expliquer** les moyens utilisés pour assurer la conformité (transparence vis-à-vis des personnes concernées), de **rendre compte** de ses activités de traitement, de les **contrôler,** et ce, afin de **garantir** la conformité. L'application du principe d'« *accountability* » introduit ainsi un mécanisme **d'autorégulation basé sur une approche par les risques.**

En contrepartie de la disparition de la plupart des formalités, le responsable de traitement (et le sous-traitant le cas échéant) doit tenir un **registre des traitements**, en pratique **rendu obligatoire pour tout organisme Hlm**[9], quel que soit son statut.

Toutefois, tout comme dans la Loi Informatique et libertés, les traitements identifiés dans le Règlement comme « ***à risques*** » continuent de faire l'objet **d'un contrôle préalable renforcé** à la fois par le DPO qui s'assure de la conduite d'études d'impact sur la vie privée (EIVP), et par la CNIL lorsque l'étude d'impact a révélé l'existence de risques importants pour les droits et libertés des personnes.

Le régime de consultation préalable de la CNIL instauré par l'article 36 du RGPD est sensiblement analogue au régime de la demande d'avis prévue aux articles 26 et 27 de la Loi Informatique et libertés pour certains traitements du secteur public, puisqu'il ne s'agit pas d'une autorisation formelle.

› La Loi Informatique et libertés pourrait être modifiée pour prévoir que le régime de la consultation préalable s'applique à d'autres cas (i.e. indépendamment du résultat de l'EIVP), voire pour maintenir un régime d'autorisation préalable dans certains cas.

En parallèle, le Règlement général relatif à la protection des données renforce la place **des codes de conduites** dans la démonstration de la conformité, ainsi que de l'utilisation **de labels et certifications** ayant fait l'objet d'une approbation par la CNIL et, le cas échant, par le Comité européen de la protection des données.

› L'obtention d'une certification ne limite pas la responsabilité du responsable de traitement, elle est toutefois prise en compte dans la démonstration de la conformité du traitement.

* Cf. Repères n°1, p.15.

9. Bien que l'obligation ne joue que pour les organismes comptant moins de 250 employés (RGPD, art.320, 5°), ce seuil ne joue pas en cas de traitements de manière habituelle de données sensibles, comme c'est le cas pour les organismes Hlm dans le cadre de l'accompagnement social personnalisé.

Les « Packs de conformité » et le RGPD

Le Règlement général relatif à la protection des données ne fait aucune référence à la démarche initiée par la CNIL en France : si les « Packs de conformité » constituent sans conteste des référentiels dont le respect permet d'assurer la licéité des traitements, **ils ne constituent pas pour le moment des codes de conduites au sens du RGPD.**
Il n'y a pas, à ce jour, de démarche de certification reprenant les **exigences précises du « Pack de conformité logement social »**. Pour autant, il constitue **un outil de référence qui a permis à de nombreux organismes d'engager leur démarche de mise en conformité, et pourrait, à terme, devenir un code de conduite.**

Conséquences

- Les traitements « ***à risques*** » pour les organismes Hlm, sont ceux déjà identifiés comme tels par la loi Informatique et libertés, en application des articles 25 à 27. Certains font l'objet d'autorisations uniques (par exemple, AU-034 et AU-035 : cf. Repères n°1 p. 20, 21). Pourraient s'ajouter de **nouveaux traitements**[10] (déjà ou nouvellement) identifiés par la loi, la CNIL ou l'organisme Hlm comme présentant des risques particuliers et devant faire l'objet d'EIVP et de formalités préalables pour les personnes concernées : *par exemple, la mise en œuvre de dispositifs reposant sur des objets connectés, des capteurs (capteurs de prévention des chutes pour les personnes âgées, capteurs se rapportant à la maîtrise de la consommation d'énergie...).*

Les organismes Hlm devront rester vigilants dans l'identification des traitements présentant des risques particuliers pour les personnes, qui ne sont pas tous visés dans le « pack conformité logement social » et pour lesquels une EIVP devra être conduite. La CNIL envisage de dispenser les traitements du « pack conformité logement social » de l'obligation de réaliser une EIVP. Pour pouvoir bénéficier de cette dispense, les organismes Hlm devront être en mesure de démontrer qu'ils **respectent en tous points les exigences posées dans le « pack de conformité logement social »**.

- Dans le cas où les traitements seraient appelés à évoluer sans que le « Pack de conformité logement social » ne soit mis à jour, les organismes Hlm seront tenus de conduire une EIVP sur le périmètre de ces évolutions.

10. Pour tous ces cas, le régime de formalités applicable devra être clarifié dans la Loi Informatique et libertés.

- Le « **Pack de conformité logement social** » est appelé à demeurer **le référentiel de base** pour les organismes Hlm. Il est possible d'anticiper que les traitements du « pack de conformité » n'auront pas à faire l'objet d'une EIVP ou de consultation préalable auprès de la CNIL (celle-ci ayant en effet le pouvoir de décider des cas dans lequels ces mesures ne sont pas requises).

  - **Le « Pack de conformité logement social » n'exonère en aucun cas les organismes du respect des dispositions du RGPD.** Ils devront, comme toute entreprise, être en capacité de démontrer qu'ils respectent l'ensemble des principes du RGPD et de la loi Informatique et libertés. Les organismes vont devoir « documenter » leurs démarches en continu. Le registre et le bilan du DPO[11] constitueront un premier outil.

- **Tous les traitements relevant du « Pack de conformité logement social » devront figurer *a minima* sur le registre**. Toute modification de traitements existants résultant d'évolutions législatives *(par exemple, introduction du NIR dans le CERFA de la demande)* auront pour effet la mise à jour du registre. Certaines pourront, le cas échéant, faire l'objet de formalités adéquates.

- **La CNIL encourage le recours à la certification et aux labels.** Les organismes auront tout intérêt à s'y référer, notamment lors du choix de nouvelles technologies ou le recours à certains systèmes de traitements suscitant – comme le « cloud computing » (informatique en nuage) par exemple – des interrogations sur leur compatibilité avec les principes de protection des données.

À NOTER

Le régime de la consultation préalable de la CNIL s'appliquera dès lors que :

- le traitement est susceptible d'engendrer des risques particuliers pour les personnes concernées (introduction de nouvelles technologies notamment, mais aussi ampleur du traitement…), et il est donc de ce fait soumis à la réalisation d'une EIVP,
- et qu'il ressort de l'étude d'impact sur la vie privée que les opérations de traitement comportent des risques élevés pour les personnes qui ne peuvent être atténués.

En cas de consultation[12], la CNIL dispose d'un délai de 8 semaines (pouvant être prorogé une fois de 6 semaines). Tout comme pour le régime actuel de la demande d'avis, l'avis est réputé favorable à défaut de réponse de la CNIL dans les délais impartis.

RGPD art. 36, 40 à 43
CNIL labels gouvernance, audit, formation
Repères n°1, p.16 à 21

11. Même s'il n'est pas prévu dans le RGPD, il est fortement recommandé d'établir un bilan annuel à destination du responsable de traitement.
12. Article 36 al 1 et 5.

LA PRISE EN COMPTE DE LA PROTECTION DES LA CONCEPTION DU TRAITEMENT DE DONNEES ET LA PROTECTION PAR DEFAUT

Le RGRP impose l'intégration des concepts de protection dès la conception (« Privacy by design ») et la protection par défaut (« Privacy by default ») lors de la mise en œuvre de tout nouveau traitement ou modification majeure d'un traitement existant en application du principe de responsabilité (« accountability »). L'implémentation de ces règles vise à assurer le plus haut niveau de protection des données à caractère personnel et constitue de ce fait l'un des éléments permettant de démontrer la conformité des traitements.

Principe

La protection des données dès la conception (*Privacy by design*) consiste en l'intégration des principes applicables à la protection des données **dès la conception** d'un traitement, puis lors de **sa mise en œuvre** et ensuite **tout au long** de son développement.

› Cela signifie que des règles et fonctionnalités doivent permettre de garantir un haut niveau de protection (exemple : le développement d'outils de gestion des habitations, des outils de purge automatique, ou la mise en place d'un dispositif de détection automatique des violations de données à caractère personnel).

La protection par défaut (*Privacy by default*) constitue le complément naturel de la protection des données dès la conception. Elle implique l'obligation pour le responsable de traitement de prendre des mesures pour assurer que **par défaut,** le paramétrage des systèmes informatiques est positionné **dans un sens assurant le plus haut niveau de protection**. L'obligation repose sur le responsable de traitement qui peut, le cas échéant, donner des instructions au sous-traitant pour en assurer la prise en compte.

› L'objectif de la protection par défaut (Privacy by default) 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).*

Conséquences

La prise en compte de la protection dès la conception et la protection par défaut est une démarche proactive visant à **anticiper les risques** (rôle préventif). Elle doit être envisagée comme **une valeur ajoutée contribuant au développement des projets informatiques** et s'inscrivant dans une démarche éthique. Elle nécessite :

- un soutien fort de la direction de l'organisme Hlm,
- une implication du DPO dès le début du projet,
- l'intégration de la prévention des atteintes à la vie privée dans la stratégie organisationnelle des organismes Hlm.

COMMENTAIRE

Pour se conformer à ce principe et assurer la conformité, les organismes Hlm devront identifier, **pour chaque traitement**, les **mesures** et procédures techniques et organisationnelles **appropriées.**

Illustration : le respect des règles de protection dès la conception par la minimisation et des durées de conservation limitées

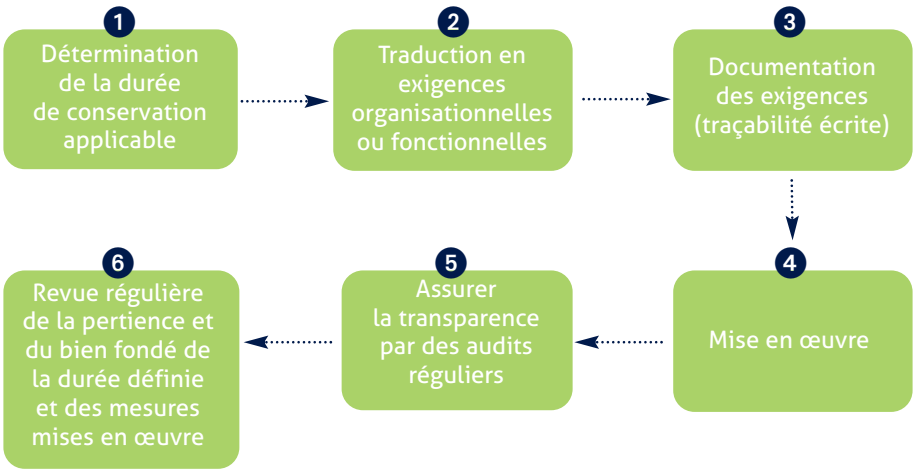
Le principe de minimisation est proche de celui de la proportionnalité, tout en étant plus exigeant. Il s'agit de recueillir le minimum d'informations et uniquement les informations nécessaires, adéquates, strictement nécessaires à la finalité poursuivie. **Le respect de ce principe engendre une nécessaire évolution des cultures professionnelles.**

Exemple 1 : la signature d'un protocole entre l'Union sociale pour l'habitat et la DGFIP en 2016
Cet accord a permis de sécuriser et de normer les échanges de données entre bailleurs sociaux et services fiscaux. Il a également permis de dresser la liste des données nécessaires, adéquates et nécessaires au regard de la finalité poursuivie. Un certain nombre d'informations précédemment collectées ont été écartées du tracé du fichier mis en place, car jugées non nécessaires à l'atteinte de la finalité poursuivie.

Exemple 2 : le respect des règles relatives aux durées de conservation
Le traitement des durées de conservation est un sujet complexe car lié à la nature des données traitées et à la finalité poursuivie. Si la notion de durée limitée de conservation est pleinement intégrée par les organismes Hlm, la mise en œuvre de durées de conservation distinctes selon la nature de la donnée ou la finalité poursuivie est délicate.

› Ces durées de conservation doivent s'appliquer à l'**ensemble des traitements, automatisés ou non**. Il est donc nécessaire de mettre en place une procédure d'archivage papier et de travailler avec l'éditeur du progiciel de gestion pour que le progiciel soit à même de permettre **la mise en cohérence la procédure d'archivage papier avec les durées de conservations des données contenues dans l'applicatif de gestion**.
Si la purge automatique est difficile à mettre en place, des solutions peuvent être trouvées par le biais des politiques d'habilitation et / ou d'anonymisation des données. *Voir les préconisations présentées dans l'espace collaboratif « informatique et libertés » du site internet de l'Union sociale pour l'habitat.*

La mise en œuvre de la minisation sur le cycle de vie des données



RGPD , art.5, 2°, art.26

1 ENCADRE

PRIVACY BY DESIGN/BY DEFAULT : LES ACTIONS À INTÉGRER DANS LES PROJETS INFORMATIQUES

Prérequis communs

› Identifier le contexte particulier applicable aux traitements de données à caractère personnel afin de déterminer les mesures les plus appropriées pour assurer la protection maximale de la vie privée et des données à caractère personnel.

› Comprendre et mettre au cœur des développements informatiques et des paramétrages les préoccupations des personnes concernées.

Protection dès la conception (Privacy by design)

› **Assurer la transparence du traitement** vis-à-vis des personnes concernées et faciliter l'exercice des droits

› **Intégrer des mécanismes** d'obtention et de retrait du consentement

› **Assurer le contrôle du traitement** par les personnes concernées : accès à des réglages permettant aux personnes concernées de minimiser le traitement de leurs données

› **Assurer une sécurité de bout en bout** :
- Mesures techniques destinées à assurer l'intégrité des données
- Prise en compte des résultats des EIVP
- Gestion fine des droits et habilitations
- Mise en place de fonctions de verrouillage des données, d'archivage, d'anonymisation ou pseudonymisation, de purge
- Réalisation régulière et l'analyse de tests d'intrusion, audits des systèmes et sous-traitants
- Documentation du référentiel de sécurité appliqué
- Sensibilisation/formation des personnels aux enjeux de sécurité

RGPD , art.25 et 45

Protection par défaut (Privacy by default)

› Établissement de **profils d'utilisateurs** par défaut

› Prévoir que **les premières interactions s'effectuent sans identification** de la personne (lors de l'accès à un service, la personne concernée ne doit pas être tout de suite obligée de divulguer ses données personnelles ; ce n'est que lorsqu'elle exprime sa volonté de s'inscrire au service, que des données d'identification pourront lui être demandées)[13]

› **Limitation des données** pouvant être saisies à celles strictement nécessaires à chaque finalité spécifique du traitement

› **Paramétrage des durées de conservation** pour que les données ne soient pas conservées sous une forme permettant d'identifier les personnes physiques au-delà de ce qui est nécessaire à la réalisation des finalités

› **Limitation de l'utilisation et du nombre** des destinataires selon les choix actifs exprimés par la personne concernée

› Possibilité de régler **le déclenchement automatique de l'archivage et des purges**

› Paramétrer tous les boutons d'options d'applications **pour qu'ils soient positionnés par défaut sur l'option la plus protectrice** des données à caractère personnel de l'utilisateur (*par exemple, un bouton autorisant le partage de données de l'utilisateur avec un autre organisme sera positionné par défaut sur « non »*).

13. Sur la plateforme web « bienvéO » permettant aux organismes Hlm de diffuser l'offre disponible, le public n'a pas à s'identifier pour accéder à l'offre. L'identification ne sera requise que pour la mise en relation de la personne avec le bailleur.

UNE NOUVELLE DEFINITION DES RESPONSABILITES EN CAS DE CO-TRAITANCE ET DE SOUS-TRAITANCE

Le RGPD introduit la notion de responsabilité conjointe, déjà présente dans le droit de l'Union, mais qui n'avait pas été transposée dans la Loi Informatique et libertés. La reconnaissance d'une responsabilité conjointe vise à responsabiliser les différents acteurs du traitement des données à caractère personnel.

Principe

Il est mis fin à la **quasi-immunité** dont jouissaient jusqu'à présent les **sous-traitants** qui se voient attribuer **une responsabilité propre.** Cependant, la personne concernée pourra toujours s'adresser au responsable de traitement qui pourra par la suite se retourner contre le sous-traitant. En effet, la répartition des responsabilités n'affecte pas le droit à réparation des personnes concernées (cf. Fiche de synthèse n°1, page 86). **La responsabilité vis-à-vis du respect de la législation** en matière de protection des données personnelles **incombe ainsi à chaque acteur** traitant des données à caractère personnel, qu'il s'agisse **d'un responsable de traitement ou d'un sous-traitant.**

Conséquences

- **Obligations en cas de responsabilité conjointe :**
  - Définition dans une convention des obligations réciproques afin d'assurer la conformité au règlement (rôle de chacun et relations vis-à-vis des personnes concernées)
  - Transparence sur cette répartition auprès des personnes concernées, notamment en ce qui concerne l'exercice des droits des personnes concernées (information, accès et rectification)
  - ***Exception*** *lorsque les obligations respectives des responsables de traitements conjoints sont définies par la loi*

- **Obligations du responsable de traitement en cas de recours à la sous-traitance :**
  - **Vérification** de la capacité du sous-traitant à assurer la mise en œuvre les mesures de responsabilité (« d'accountability »)

  - **Actualisation des contrats** de sous-traitance* qui sont écrits et doivent :
    - **Définir** l'objet et durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel, les catégories de personnes concernées, les droits et obligations du responsable de traitement et du sous-traitant.
    - **Prévoir** la possibilité de contrôler et vérifier le respect du contrat et de la Législation relative à la protection des données à caractère personnel par le sous-traitant principal, ainsi que les sous-traitants ultérieurs.
    - **Mettre à disposition** du responsable de traitement toutes les informations nécessaires à la réalisation d'audits et à la tenue de la documentation relative aux traitements.
    - **Prévoir que le sous-traitant alerte** le responsable de traitement en cas de violation des données à caractère personnel.
    - **Comporter les instructions documentées** du responsable de traitement notamment en matière de sécurité.

* Cf. Modèle de contrat de sous-traitance sur l'espace collaboratif « Informatique et libertés » www.union-habitat.org

Illustration

- **Situations de responsabilité conjointe (des données personnelles identiques sont collectées ou traitées pour des finalités différentes ou propres à chaque responsable de traitement) :**
  - Utilisation du fichier des locataires par une filiale chargée de promouvoir l'accession sociale.
  - Les systèmes particuliers de traitement automatisé (fichiers partagés de gestion de la demande pour lesquels les organismes Hlm sont responsables du traitement des données en tant qu'utilisateurs aux côtés de l'État qui a la responsabilité globale du dispositif du SNE).

- **Situations de sous-traitance**
  - Réalisation d'une enquête confiée à un prestataire se présentant comme l'organisme Hlm et réalisant l'enquête sur la base d'une grille d'information et suivant la marche à suivre et les conditions techniques et de sécurité précises données par l'organisme Hlm.
  - Prise en main à distance par le prestataire chargé de la maintenance informatique.

- **Situations complexes**
  - Certaines situations peuvent nécessiter une approche au cas par cas. Par exemple, lorsque le bailleur finance une mesure d'accompagnement social, l'organisme Hlm peut se trouver en situation de responsable unique du traitement (cas dans lequel l'exécution de la mission implique le traitement de données par le prestataire pour le compte de l'organisme). Dans d'autres cas, l'association menant la mesure peut être qualifiée de responsable de traitement. Dans de telles situations, il importe **d'impliquer le délégué à la protection des données** (DPO) afin de déterminer la qualification applicable et ses implications sur le contenu du contrat conclu avec l'organisme tiers.

2 ENCADRE

OBLIGATIONS RESPECTIVES DES RESPONSABLES DE TRAITEMENT ET DES SOUS-TRAITANTS

Obligations du responsable de traitement	Obligations du sous-traitant	Obligations communes
› Respect des principes / répartition transparente des responsabilités en cas de responsabilité conjointe (contrat) › Mise en œuvre du « *Privacy by default* » / « *Privacy by design* » › Conduite d'EIVP › Contrôle du recours à la sous-traitance › Notification des violations de sécurité à l'autorité de protection des données › Consultation préalable de l'autorité de contrôle	› Obligation de réparation en cas de préjudice dû à la violation du règlement, uniquement s'il n'a pas respecté les obligations imposées aux sous-traitants par le règlement ou les instructions du responsable de traitement › Ne peut pas recruter un autre sous-traitant sans l'autorisation écrite préalable du responsable de traitement › Notification au responsable de traitement en cas de violation de données dans les meilleurs délais	› Désignation d'un DPO/Coopération avec les autorités › Sécurité du traitement › Respect des règles relatives aux transferts › Désignation d'un représentant si non établi sur le territoire de l'UE › Tenue du registre des activités de traitements › Respect des codes de conduite /certifications

3

ENCADRE

FAISCEAU D'INDICES POUR DÉTERMINER LA QUALIFICATION JURIDIQUE DU PRESTATAIRE

Critères de qualification	En faveur de la qualification de sous-traitant	En faveur de la qualification de responsable de traitement
› Le niveau des instructions préalables données par le responsable de traitement	› Les instructions, notamment concernant les mesures de sécurité et modalités de traitement (moyens) sont détaillées dans le contrat ou les directives données au cours de son exécution et présentent un niveau d'exigence particulier	› Le prestataire dispose d'une large autonomie dans la détermination des moyens du traitement ou uniquement d'instruction générale
› Le niveau du contrôle de l'exécution des prestations	› La prestation est surveillée en détail par l'organisme Hlm qui réalise des audits réguliers et lui demande des comptes sur l'exécution › Les données de l'organisme Hlm sont séparées des données des autres clients du prestataire	› L'organisme Hlm ne surveille pas la réalisation de la prestation, il n'a pas de pouvoir d'audit › Le prestataire peut utiliser les données à caractère personnel pour ses propres besoins/finalités › Les données de l'organisme Hlm sont mutualisées avec celles des autres clients du prestataire
› La transparence	› L'identité du prestataire n'est pas connue par les personnes concernées › Il se présente au nom de l'organisme Hlm › Le droit d'accès aux données traitées s'exerce auprès de l'organisme Hlm	› L'identité du prestataire est connue par les personnes concernées › Il se présente en tant que tel › Le droit d'accès aux données traitées par le prestataire s'exerce auprès du prestataire
› L'expertise	› Le prestataire utilise l'infrastructure technique de l'organisme Hlm client ou celles mise à disposition par l'organisme Hlm pour réaliser sa prestation	› Le prestataire est expert sur son domaine d'intervention et impose la réalisation de la prestation sur sa propre infrastructure (*l'organisme Hlm n'a pas de pouvoir de négociation, ne peut les modifier parce qu'il n'a pas les compétences, ou parce que l'outil ne fait pas l'objet d'un développement spécifique*)

RGPD, art 28 et 29
CNIL, rapport sur l'externalisation, 2009
G29, WP 169

Seule la réalisation de plusieurs de ces critères qui constituent des faisceaux d'indices permettra de qualifier le prestataire. L'appréciation devra être effectuée au cas par cas.

LE RENFORCEMENT DES EXIGENCES CONCERNANT LES DROITS DES PERSONNES : NOUVELLES EXIGENCES DE TRANSPARENCE

Si les règles relatives à l'information et aux droits des personnes sont reconduites, le RGPD met l'accent sur l'obligation de transparence qui doit permettre à la personne concernée de maîtriser la manière dont sont traitées ses données à caractère personnel.

Principe

Le RGPD introduit une **obligation d'efficacité, de diligence et de vigilance** du responsable de traitement qui doit prendre toutes mesures pour faciliter l'exercice des droits d'accès et de rectification. **Des obligations de clarté et de transparence s'appliquent par ailleurs pour le droit à l'information.** Le RGPD incite au recours à des notices éventuellement **accompagnées d'icônes normalisées** afin d'assurer une meilleure compréhension de tous (*ces icônes ne sont pas encore disponibles*).

Conséquences

Dans l'information des **personnes concernées**, les organisme Hlm doivent s'assurer de :

- **la mise à jour** des mentions d'information présentes sur l'ensemble des formulaires, documents et sites comportant des données à caractère personnel, le cas échéant, *via* des icônes ;
- **en cas de responsabilité conjointe,** que les obligations respectives de chaque responsable de traitement vis-à-vis des personnes concernées soient bien identifiées.

Illustration

L'insertion d'une clause « informatique et libertés » dans le contrat de location* précisant l'utilisation des données à caractère personnel des locataires **dans le cadre de la gestion courante,** est l'un des moyens les plus sûrs pour satisfaire à l'obligation d'information. Il est également possible de prévoir la remise au locataire d'un document séparé contre signature (afin de prouver l'information) ou l'envoi d'un courrier.

En revanche, dès lors que le traitement repose sur le recueil du consentement (données de santé), le bail ne peut servir de support. Le recueil du consentement doit s'exercer au moment du traitement de la situation. **Concernant les données de santé, l'annexe « handicap » du CERFA dûment complétée par la personne, vaut consentement lors d'une demande de logement.**

À NOTER

La notice d'information doit être **visible, accessible, compréhensible, concise.** Elle doit être rédigée en termes **clairs et simples**.

› Voir annexe page 83, le contenu des mentions d'informations.

* Modèle de clause à insérer dans le bail (espace collaboratif Informatique et liberté de l'USH)

4

ENCADRE

LES RÈGLES D'INFORMATION EN CAS DE COLLECTE INDIRECTE

Rappel

Cas de collecte directe
- Formulaire d'état des lieux rempli par le locataire
- Données collectées sur l'intranet espace réservé au locataire
- Inscription sur le site de l'organisme Hlm à une liste de diffusion (journal locataires)

Cas de collecte indirecte
- Données reçues de la CAF
- Acquisition par une entité du groupe de l'organisme Hlm d'une liste de locataires à démarcher pour l'accession à la propriété
- L'organisme Hlm recueille les éléments du CERFA non saisis par lui-même.

En cas de collecte indirecte, l'information des personnes par l'acquéreur des données doit intervenir :
- dans un délai raisonnable après avoir obtenu les informations (1 mois) ;
- lors de la première communication avec la personne concernée.

Lorsque la communication des données n'est pas prévue par la loi, le responsable de traitement ayant collecté directement les données doit informer la personne concernée sur la communication éventuelle/possible à un tiers et ses finalités ; préalablement à la collecte, elle doit avoir obtenu, soit le consentement de la personne concernée (par exemple en cas de données sensibles), soit lui avoir permis de s'opposer à une telle communication.

L'organisme Hlm doit s'assurer du caractère suffisant de l'information dont dispose la personne concernée sur le traitement opéré par l'organisme Hlm. Cette information peut se faire par les mentions contenues dans le bail. Les conventions conclues dans le cadre de la cotraitance pourront mettre à la charge du cotraitant l'information des personnes concernées par les traitements mis en œuvre par l'organisme Hlm.
Par exemple :
- **données disponibles dans le SNE :** lorsque le bailleur accède aux données d'un demandeur de logement ayant saisi lui-même sa demande ou par le biais d'un autre guichet d'enregistrement, la collecte est indirecte. La personne concernée est informée de l'utilisation possible des ses données par l'organisme Hlm dans l'attestation de dépôt de sa demande ;
- **données transmises par la CAF** : mention dans la quittance de la prise en compte des données transmises par la CAF.

AUTRE EXEMPLE

Lors du lancement d'une enquête portant sur l'occupation du parc social, un organisme a souhaité mieux identifier la situation et les besoins de ses locataires âgés. Pour ce faire, un questionnaire a été travaillé avec la CARSAT locale et joint aux formulaires de l'enquête OPS. Les locataires âgés ont été informés du caractère facultatif de leurs réponses et de la nature de la finalité poursuivie.

RGPD, art. 12 et 13

LE RENFORCEMENT DES EXIGENCES CONCERNANT LES DROITS DES PERSONNES : NOUVELLES EXIGENCES RELATIVES AU CONSENTEMENT

Outre des mentions d'information revisitées, les organismes vont devoir être attentifs aux modalités de recueil et de retrait du consentement. Le RGPD introduit de nouvelles règles applicables au consentement visant à garantir la manifestation d'une véritable liberté de droits de la personne concernée.

Principe

Le consentement doit être non seulement libre et spécifique, mais également **éclairé et univoque** et doit se manifester par **une déclaration ou un acte positif clair.** La personne concernée doit être informée de la possibilité de retrait du consentement et des conséquences du retrait. La notion de consentement dans le RGPD implique l'existence **d'une véritable liberté de choix** qui se manifeste **par l'absence de préjudice** en cas de **retrait du consentement**.

› Le fait que le consentement soit requis pour traiter certaines catégories de données à caractère personnel (santé notamment) ne préjuge pas du fondement légal du traitement. Ainsi, si les traitements à des fins de suivi personnalisé sont fondés sur la réalisation de la mission d'intérêt public de l'organisme, le consentement reste nécessaire lorsque la loi n'a pas expressément prévu que des données particulières doivent être traitées dans ce cadre.

Conséquences sur le recueil du consentement

- Revoir les conditions de recueil du consentement afin d'assurer un consentement éclairé et informer sur la possibilité de retrait du consentement. Le consentement peut prendre différentes formes : formulaire de recueil, déclaration écrite (y compris électronique) ou orale ou case à cocher (non pré cochée).

- Dès lors que le traitement concerné repose sur le recueil du consentement et conformément au principe de responsabilité (« accountability »), le responsable de traitement doit être en capacité à tout moment d'attester que le consentement a bien été recueilli. **La charge de la preuve du consentement pèse sur le responsable de traitement**.

Pour approfondir

- **Les critères de qualité du consentement**
  - Il ne doit pas être recueilli globalement ;
  - Il ne doit pas être recueilli en même temps qu'une autre déclaration ou que l'acceptation des conditions générales ou du contrat ;
  - L'information donnée doit identifier de manière détaillée les finalités.

- **Cas où le consentement ne peut servir de fondement légal du traitement**
  - **Lorsque la personne concernée ne dispose pas d'une véritable liberté de choix** (cas de collecte par une autorité publique par exemple) ; n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice ;
  - **en présence d'un déséquilibre manifeste** entre la personne concernée et le responsable de traitement ;
  - **lorsque le consentement a été forcé** (cas dans lequel le consentement au traitement de données est lié à l'acceptation des conditions générales du service, alors que le consentement porte sur une option facultative ou sur un traitement de données non nécessaire à l'ouverture du service ; ou encore **s'il vise à déroger à une disposition du règlement.**

Mesures pratiques à mettre en œuvre pour assurer le respect du consentement

- Déterminer les moyens pratiques qui vont être mis en œuvre pour obtenir le consentement des personnes concernées.
- S'assurer que le traitement ne puisse pas être mis en œuvre sans consentement
- S'assurer que le consentement sera obtenu de manière libre.
- S'assurer que le consentement sera obtenu de manière éclairée et de façon transparente quant aux finalités du traitement.
- S'assurer que le consentement sera obtenu de manière spécifique à une finalité.

RGPD, 32ème Cons. , art.7

LES MODIFICATIONS APPORTÉES A LA PROCÉDURE DE GESTION DES DEMANDES DES PERSONNES À L'ACCES AUX DONNÉES

Le RGPD améliore les procédures de gestion des demandes d'accès aux données par les personnes concernées (accès, rectification...).

Principe

- Nouvelles modalités de communication
  - Lorsque la demande est présentée par voie électronique, le responsable de traitement doit s'assurer de l'identité de la personne concernée et doit lui fournir les informations électroniquement de manière sécurisée, à moins que la personne concernée ne demande qu'il en soit fait autrement.
- **Raccourcissement des délais** à respecter par le responsable de traitement **pour répondre à une demande de droit d'accès**
  - **Principe** « **dans les meilleurs délais** » avec délai maximum **d'un mois** à compter de la réception de la demande (au lieu de 2 mois).
  - **Possibilité de prolongation de deux mois** si la demande relève d'un caractère « complexe » qui devra être notifié à la personne concernée. Le responsable de traitement devra en exposer les raisons dans un délai d'un mois à compter de la réception de la demande.
  - **Vérifications à effectuer :** en cas de doute, le responsable de traitement doit conduire des vérifications sur l'identité de la personne concernée. La réponse adressée à cette dernière est l'occasion de lui rappeler des droits complémentaires, comme le droit à la saisie de l'autorité de la CNIL (droit à réclamation).
- **Aucun paiement ne peut être demandé**, contrairement à ce que prévoit la Loi Informatique et libertés, **sauf en cas de demandes répétées**.

Conséquences

Les organismes Hlm doivent mettre en place ou revisiter la procédure de gestion des demandes de droits d'accès et rectification, et respecter les délais de réponse requis.

RGPD, art.12.1 et 13.2, art. 15 et 16

PARTIE 4

Les nouveaux outils de la conformité

LE RÔLE CENTRAL DU DPO DANS LA CONDUITE DE LA DÉMARCHE

Avec le règlement général relatif à la protection des données (RGDP), le correspondant Informatique et Libertés (CIL) prévu dans la Loi Informatique et libertés devient le délégué à la protection des données (généralement identifié sous l'acronyme « DPO » ou « Data Protection Officer »).

Principe

Du CIL au DPO : un changement de posture

Sans être totalement bouleversé (cf. Repères n°1 p.14), le statut du DPO est sensiblement différent de celui du CIL (cf. fiche de poste, annexe, p. 80). Cette évolution – qui n'est pas que sémantique – marque le franchissement d'une étape et fait du DPO une fonction centrale et stratégique dans la mise en place de l'organisation appropriée pour assurer la conformité à la législation en matière de protection des données personnelles. La désignation du DPO paraît d'autant plus nécessaire si l'on tient compte du besoin d'expertise résultant de la complexité des nouvelles règles découlant du RGDP.

Des organismes Hlm soumis à l'obligation de nomination

Sa désignation est ainsi rendue **obligatoire** pour les organismes du secteur public (critère organique) ou lorsque les traitements mis en œuvre entraînent, **au titre des activités principales du responsable de traitement** :

- du fait de leur nature, de leur portée et/ou de leurs finalités, **un suivi régulier et systématique des personnes à grande échelle** ;
- **le traitement à grande échelle de données sensibles** ou relatives à des infractions, condamnations ou mesures de sûreté.

Les précisions apportées par le G29 dans ses lignes directrices

- Le suivi est « **régulier** » si les données sont traitées à intervalles réguliers, ou de manière constante ou périodique.
- Le suivi est « **systématique** » si les données sont traitées selon un système ou une stratégie prévus et organisés dans le but de collecter des données.
- Pour déterminer si le traitement est « **à grande échelle** », il faut tenir compte de différents facteurs : le nombre de personnes concernées par les traitements, le volume de données traitées, la durée du traitement, et l'étendue géographique du traitement...

Le DPO pourra être **externalisé ou mutualisé** sans limite de seuil. Il sera toutefois nécessaire de prévoir **le pilotage en interne de la mission** par la désignation de relais.

Il assure pleinement un **rôle de médiateur** puisque les personnes concernées peuvent le saisir directement, ses coordonnées devant être rendues publiques. Il est amené à jouer **un rôle essentiel dans la diffusion d'une culture d'approche par les risques** dans **l'ensemble de l'organisme Hlm.**

Même lorsque sa désignation n'est pas obligatoire, il peut être recommandé de le faire, car il s'agit d'un gage de la volonté d'assurer la conformité, facteur de confiance auprès des parties prenantes. Le DPO est également un **facilitateur** dans le déploiement des projets informatiques et dans l'accompagnement de l'innovation.

› La loi informatique et libertés pourra par ailleurs prévoir d'autres cas de désignation obligatoire du DPO.

› Sa désignation n'entraîne **aucun allégement dans l'application de la législation** en matière de protection des données personnelles : il s'agit d'une **garantie supplémentaire** afin d'assurer le respect de la législation.

LES MISSIONS DU DPO

G29, lignes directrices WP 243 et 248

Conséquences

Au regard des critères définis par le RGDP, **la désignation d'un DPO devrait être rendue obligatoire** pour les organismes Hlm, dans la mesure où ces derniers sont amenés, au titre de leur mission de service public, à traiter de données sensibles ou à mettre en œuvre des systèmes de profilage (cotation) à plus ou moins grande échelle.

Pour les organismes qui le souhaitent, le DPO pourra être **mutualisé** au sein d'un groupe ou **externalisé** auprès d'un prestataire, sous réserve du maintien de la proximité (*proximité géographique ou facilité à être joint*) du DPO avec les organismes Hlm l'ayant désigné. Il doit en effet être facilement joignable par chaque organisme, mais également par les personnes concernées. Il doit également être en mesure d'accompagner les équipes opérationnelles sur le terrain .

En cas d'externalisation, les organismes Hlm devront prévoir la conclusion **d'une convention de services** encadrant précisément les conditions d'intervention et les missions du prestataire. En fin de mission, les organismes devront prévoir les conditions de réversibilité, notamment la restitution du registre dans un format permettant une exploitation immédiate par les organismes Hlm concernés.

5 ENCADRE

SYNTHÈSE DU RÔLE DU DPO

La mise en place de la fonction de délégué à la protection des données (DPO) nécessite d'être anticipée et organisée, afin d'être prêt en mai 2018.

Le délégué à la protection des données (DPO) est le successeur naturel du CIL. Les personnes désignées en tant que correspondant Informatique et Libertés (CIL), sous réserve de remplir les nouvelles exigences statutaires, ont vocation à devenir délégués à la protection des données en 2018, et sous réserve de leur désignation effective par leur organisme de rattachement *(via un formulaire mis à disposition sur le site de la CNIL).*

Pour garantir l'effectivité de ses missions

- Le DPO doit disposer de qualités professionnelles et de connaissances spécifiques,
- il doit être à l'abri des conflits d'intérêts (ne peut être juge et partie)
- il doit bénéficier de moyens matériels et organisationnels, de ressources, à adapter selon la taille, la structure et l'activité de l'organisme, et du positionnement lui permettant d'exercer ses missions avec efficacité.
- il n'est pas personnellement responsable en cas de non-conformité de son organisme avec le règlement.
- il peut être **externalisé :** les organismes Hlm devront toutefois s'assurer que les missions du DPO telle que définies dans la convention de services correspondent bien à leurs besoins au regard des moyens dont ils disposent pour assurer le relais en interne.

La feuille de route du DPO pour préparer l'organisme à l'application du RGPD

- finaliser l'inventaire des traitements de données personnelles mis en œuvre ;
- évaluer les pratiques de l'organisme Hlm et assister les directions dans la mise en place des procédures (audits, « privacy by design », notification des violations de données, gestion des réclamations et des plaintes, etc.) ;
- assister l'organisme Hlm dans l'identification des risques associés aux opérations de traitement ;
- mettre à jour la politique de protection des données personnelles de l'organisme Hlm ;
- sensibiliser les opérationnels et la direction sur les nouvelles obligations.

TÉMOIGNAGE

Malika EL ABED, directrice de projet Informatique et Libertés, CIL Nantes Métropole Habitat depuis 2015*

La mise en place du RGPD

Le RGPD est une bonne chose. Il renforce les libertés individuelles.

Les individus sont en effet mieux armés pour faire face aux bouleversements numériques.

Pour les organismes Hlm, l'approche par les risques permet aux directions générales d'assurer plus facilement la mise en conformité des traitements.

Premières actions et réalisations

- Réalisation d'un audit par un prestataire externe.
- Appropriation des conclusions pour déterminer un plan d'actions personnalisé et insertion des actions de conformité identifiées dans les procédures existantes.
- Conduire des études d'impacts sur la vie privée (EIVP) afin de s'approprier la méthodologie
- Poursuivre les actions de formation auprès de l'ensemble des personnels avec une approche métiers.

Méthodologie déployée

- Mise en place de sessions de sensibilisation pour les nouveaux arrivants, ainsi que pour les cadres.
- Construction d'un « processus de la donnée » incluant les politiques de protection de la vie privée et de sécurité.
- Mise en place d'une gouvernance à 2 niveaux :
  - un COPIL « informatique et libertés »se réunissant deux fois par an ;
  - un comité technique « informatique et libertés » se réunissant tous les trimestres.

Conseils aux futurs DPO

- Assurer sa légitimité au sein de l'organisme à travers la validation de la Direction Générale
- Structurer et organiser l'action du DPO et mettre en place la gouvernance de la donnée
- Impliquer tous les services concernés afin de ne pas agir seul
- Structurer et organiser l'action du DPO et mettre en place la gouvernance de la donnée
- Intégrer le RGPD dans les processus métiers et lier toute la politique de sécurité du DSI au RGPD.

* OPH, 25 000 logements, 600 collaborateurs

À RETENIR

Des missions renouvelées et renforcées

- Une implication systématique du DPO dans les projets : le DPO devra être consulté et accompagnera en pratique les équipes opérationnelles dans la réalisation des études d'impact et veillera à la réalisation des analyses de risques (soit par les responsables sécurité informatique internes à l'organisme soit en préconisant le recours à un expert sécurité externe).
- Des moyens renforcés pour la réalisation de ses nouvelles missions : formation, temps nécessaire, ressources financières, équipe...
- Il sera un interlocuteur privilégié en cas de violation de données personnelles.
- Un levier pour que les demandes de droit d'accès soient satisfaites en un mois (au lieu de deux mois actuellement).
- Un interlocuteur privilégié des personnes concernées sur l'exercice de leurs droits ou en cas de réclamation portant sur la façon dont leurs données à caractère personnel sont traitées par l'organisme Hlm.

De nouveaux moyens d'action

- Un positionnement lui permettant d'être proche de la direction de l'organisme Hlm.
- Le DPO devra disposer de l'accès direct aux données à caractère personnel et aux opérations de traitement, aux fins de lui permettre d'instruire les plaintes et réclamations dont il est saisi.
- Une connaissance experte de la législation en matière de protection des données personnelles (adaptée à la sensibilité des traitements mis en œuvre par l'organisme) confortée par de la formation continue.

Comment s'y préparer ?

- S'ils le souhaitent, les CIL en poste pourront être confirmés dans leur fonction en tant que DPO dès lors qu'ils justifient de l'expertise acquise et d'un positionnement suffisant.
- Pour les organismes Hlm n'ayant pas de CIL, les personnes pressenties pour le poste devraient pouvoir bénéficier d'une formation (de préférence certifiante) en vue de pouvoir justifier de leur expertise.
- En cas de mutualisation ou d'externalisation, les organismes devront mettre en place des référents internes.
- Il conviendra d'identifier les moyens (budgétaires, humains, matériels, formations) nécessaires à l'exercice de la mission du DPO.
- Les organismes Hlm devront communiquer les coordonnées du DPO sur leur site internet, leurs formulaires, etc.
- La CNIL mettra à disposition un formulaire en ligne pour passer du rôle de CIL à celui de DPO.

Voir également en annexe : les différences statutaires CIL/DPO : page 40
exemple de fiche de poste du DPO : page 80

GDPR, 97ème Cons. art. 37 à 39,
G29, lignes directrices WP 243 et 248
CNIL, label gouvernance

LE CONTRÔLE RENFORCÉ DU FONDEMENT LÉGAL

Le Règlement confirme l'obligation pour les responsables de traitements de justifier de l'existence d'un fondement légal pour traiter des données à caractère personnel. Il clarifie pour le secteur public les cas dans lesquels les différents fondements peuvent s'appliquer.

Principe

- Les traitements mis en œuvre par les organismes Hlm **sont en général justifiés** par l'un des **fondements suivants :**
  - l'exécution d'une **mission d'intérêt public** ou relevant de l'exercice de l'autorité publique *(exemple : le suivi social)*
  - le respect d'une **obligation légale** *(exemple : mise en œuvre de la gestion partagée dans le cadre de la loi égalité/ citoyenneté)*
  - la **nécessité contractuelle** *(exemple : respect des obligations du locataire contenues dans le bail).*

- **De façon accessoire, ces traitements peuvent reposer sur d'autres fondements,** :
  - le consentement,
  - ou 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, (*exemple : l'amélioration de la qualité des services est un intérêt légitime pour les organismes Hlm, mais il ne doit pas conduire à une intrusion excessive dans la vie privée des locataires, faute de quoi il devrait reposer sur un autre fondement, comme le consentement).*

Conséquences

- Les organismes Hlm devront vérifier que **les traitements existants** s'inscrivent dans l'un des fondements identifiés par le RGDP et devront documenter l'évaluation effectuée pour chaque finalité.

- S'agissant du **consentement,** il n'a vocation à servir de fondement aux traitements mis en œuvre pour les organismes Hlm que **lorsque aucun autre fondement n'est applicable**, par exemple pour l'utilisation de données dans le cadre de prestation facultative (*exemple : adhésion à un contrat d'assurance habitation proposé par le bailleur*).

- Le consentement est parfois exigé comme **condition supplémentaire** applicable au traitement de certaines données : dans pareille hypothèse, il ne sert pas de fondement au traitement mais permet la collecte de données qui ne pourraient pas être traitées sans le consentement de la personne concernée (*exemple : données de santé dans le cadre de la gestion d'une demande de mutation*).

6 ENCADRE

L'IDENTIFICATION DE LA BASE LÉGALE DES TRAITEMENTS

Finalité des traitements du Pack conformité logement social	Contexte légal de la mise en œuvre du traitement
› Gestion des demandes de logement social	› Mission de service public
› Gestion de l'attribution des logements sociaux	› Mission de service public
› Suivi social personnalisé	› Mission de service public (*avec consentement spécifique pour la collecte de données relatives à la santé*)
› Gestion de la conclusion, exécution et fin du contrat de location *(état des lieux, appels de loyers, quittances et règlements)*	› Conclusion et exécution des contrats
› Gestion et entretien des immeubles	› Conclusion et exécution des contrats
› Vidéosurveillance, contrôle d'accès	› Intérêt légitime du bailleur d'assurer la sécurité des biens et des personnes
› Gestion des troubles anormaux de voisinage, gestion des réclamations, plaintes	› Obligation contractuelle du bailleur d'assurer une jouissance paisible. Intérêt légitime du bailleur de prévenir les atteintes au patrimoine et aux personnes
› Information/prospection permettant de faire connaître aux locataires les programmes d'accession sociale de l'organisme Hlm	› Intérêt légitime de l'organisme Hlm d'organiser les parcours résidentiels et obligation légale en cas de mise en vente de logement sociaux (vente Hlm)
› Suivi des dépenses énergétiques des locataires	› Consentement

RGPD, art. 5

LA MISE EN ŒUVRE DU « PRIVACY BY DESIGN » ET « BY DEFAULT »

Le RGPD renforce la nécessité d'être particulièrement vigilent sur la nature des données collectées au regard de la finalité poursuivie. Il s'agit de collecter uniquement les données nécessaires à l'accomplissement des missions.

Principe de minimisation

Le respect du principe de minimisation permet d'une certaine manière de minimiser le risque. Plus le nombre de données collectées et traitées est faible, plus le risque de détérioration ou de violation de la donnée est limité.

Une autre manière de se sécuriser consiste à rendre les données anonymes ou à les pseudonymiser. Les **données anonymes**, ou les données **rendues anonymes** ne relèvent pas par principe de la législation informatique et liberté, à la condition toutefois d'être « suffisamment anonymisées » (cf. encadré n°7, page 44).

› **Les données sont considérées comme anonymes lorsque l'identification de la personne concernée, directement ou indirectement, devient impossible que ce soit par le responsable du traitement ou par un tiers.** Toutefois les exigences posées par le règlement et leur interprétation par les autorités de protection des données (ainsi que la jurisprudence) rendent **le constat de l'anonymat très difficile**, et aléatoire.

› Les moyens d'anonymisation mis en œuvre doivent permettre d'éviter toute réidentification compte tenu des moyens « raisonnables » que le responsable ou les tiers seraient prêts à mettre en œuvre à cette fin, y compris à des fins répressives.

› Les données anonymes doivent être distinguées des données **pseudonymes**. En effet, la notion de « **pseudonymisation** » renvoie à l'usage de procédés de traitements de données à caractère personnel destinées à rendre impossible la réattribution des données sans avoir recours à des données complémentaires détenues par un tiers (*exemple : principe d'une table de correspondance détenue par un tiers de confiance*).

Des données à caractère personnel agrégées à **un niveau suffisant tenant compte de l'évaluation des risques d'identification directe ou indirecte**, constituent des données pseudonymes.

À NOTER

Le fait de chiffrer les données – apprécié comme une mesure de protection de la confidentialité– n'altère pas la nature des données qui demeurent des données à caractère personnel. Les données chiffrées sont des données pseudonymes soumises à la législation Informatique et liberté.

Conséquences

La question de l'anonymisation s'est récemment présentée dans le cadre de l'application de la loi Égalité et citoyenneté du 27 janvier 2017 concernant l'exploitation des données de l'enquête OPS. La finalité poursuivie est de contribuer à alimenter des réflexions locales conduisant à la définition d'orientations d'attributions et de plans de gestion partagée de la demande.

Une note de cadrage* a été produite à destination des organismes Hlm : à défaut d'anonymisation, il a été proposé de « secrétiser » les données et de mettre en place un contrat avec le sous-traitant prévoyant des conditions très strictes de sécurité et de destruction des données brutes.

7 ENCADRE

DONNÉES ANONYMES : ÉLÉMENTS D'APPRÉCIATION POUR ÉVALUER LE RISQUE DE RÉ IDENTIFICATION

Éléments contextuels pertinents

- Mesures de sécurités mises en place
- Taille et nature des données
- Moyens de communication envisagée de données à des tiers
- Coût de l'identification
- Sensibilité de la donnée (*exemple : maladie rare*)
- Le temps nécessaire à la ré identification
- Les technologies disponibles au moment du traitement et leurs évolutions
- Le caractère légal des moyens permettant d'accéder à l'information complémentaire permettant l'identification

Exemple de techniques et procédés permettant l'anonymisation

- **L'anonymisation par randomisation :** cette option consiste à modifier les valeurs réelles pour empêcher que les données anonymisées puissent être mises en relation avec les valeurs originales. On peut ajouter des techniques supplémentaires, tel que le « bruit » ou la permutation (méthode consistant à mélanger les valeurs des attributs dans un tableau qui liera des personnes non concernées par l'information).

- **L'anonymisation par généralisation, ou l'agrégation des données :** méthode qui consiste à étendre le champ visé par l'information ou d'enlever un degré de précision à certains champs.

La CNIL s'apprête à certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification de la conformité de processus d'anonymisation des données à caractère personnel, notamment en vue de la réutilisation d'informations publiques (open data).

*espace collaboratif Informatique et libertés : www..union-habitat.org/

8

ENCADRE

DONNÉES PSEUDONYMES : LES CONDITIONS À RÉUNIR POUR CONSIDÉRER QUE DES DONNÉES SONT PSEUDONYMISÉES

Éléments contextuels pertinents :

- Les données complémentaires permettant l'identification doivent être conservées séparément des données pseudonymisées.
- Elles doivent être conservées dans les conditions techniques et organisationnelles empêchant la réattribution.

Exemple de techniques et procédés permettant la pseudonymisation

En pratique lorsque les informations sont pseudonymisées, les identifiants sont remplacés par un pseudonyme. Ceci peut se faire par le biais :

- **du cryptage à clé secrète**, il est donc possible de ré identifier une personne en recourant à une table de correspondance. La technique de cryptage de l'identité de la personne concernée est particulièrement utile dans le cadre de la recherche scientifique ou historique, quand des responsables de traitement doivent s'assurer qu'ils s'intéressent aux mêmes personnes, mais où ils n'ont pas besoin de connaître les véritables identités des personnes concernées.

- **du « hachage »** (procédé de chiffrement irréversible) **avec SEL** (un SEL désigne l'ajout de caractères ou autres données avant le calcul de l'empreinte résultant du « hachage ») ou par le biais d'une combinaison des techniques de **« hachage » et de « salage »** (le salage étant utilisé pour contrer les attaques par dictionnaires.).

- **de la « Tokenization »** qui sépare l'information du code qui la caractérise. La technique repose sur l'application de mécanismes de chiffrement à sens unique ou sur l'assignation d'un numéro séquentiel ou d'un nombre produit de manière aléatoire qui n'est pas mathématiquement dérivé des données originales (*généralement utilisé par les systèmes de paiements*).

L'appréciation doit se faire au cas par cas sur chaque jeu de données à pseudonymiser.

RGPD : 26ème et 29ème Cons., art. 4,5° et 25§1
CJUE 19 oct. 2016, C-581/14, Breyer
CE, 8 fév. 2017, n° 393714, JC Decaux c/ CNIL
G29 : WP 136 et 216

L'EXIGENCE DE RIGUEUR DANS LE RESPECT DES DURÉES DE CONSERVATION ET DE MISE EN ŒUVRE DU « DROIT A L'OUBLI »

Le RGPD redéfinit le droit à l'oubli en distinguant, d'un côté le droit à l'effacement (*nouveau « droit à l'oubli »*) et de l'autre, le droit à la limitation du traitement. Il consacre également le « droit à l'effacement numérique » ou « droit au déréférencement », consacré par l'arrêt de la CJUE du 13 mai 2014 Google Spain[14].

Principe

L'exercice du droit à l'effacement s'articule avec le droit d'opposition qui est lui-même revu dans ses modalités d'exercice et dans ses conséquences.

- **Articulation avec le droit d'opposition :** le droit à l'effacement peut être une des conséquences de l'exercice du droit d'opposition. La différence principale avec la Loi Informatique et libertés est qu'il n'appartient plus à la personne concernée de justifier d'un intérêt légitime pour exercer son droit d'opposition. Au contraire, **le RGDP opère un renversement de la charge de la preuve : c'est au responsable de traitement de justifier de l'existence d'un ou de « *motif(s) légitime(s) impérieu(x)* »** pour continuer à traiter les données.

  - Il est reconnu aux personnes concernées, au même titre que le droit à la tranquillité permettant de s'opposer à la prospection commerciale, un droit d'opposition **au profilage à des fins commerciales**, le profilage intervenant avant la phase de sollicitation.

Illustration

- **Le droit à l'oubli /droit à l'effacement** survient lorsque :
  - à l'issue de la période d'archivage courant ou intermédiaire, lorsque la conservation des données n'est plus nécessaire à la finalité et que le responsable de traitement ne peut pas justifier d'une obligation légale de conserver les données ou d'autre fondement juridique justifiant leur conservation.
  - En cas d'opposition de la personne concernée, lorsque le responsable de traitement ne peut justifier d'un motif légitime impérieux pour conserver les données.

Exemple : obligation d'effacer les données sensibles collectées sans consentement de la personne.

- **Le droit à la limitation** survient lorsque :
  - il y a contestation de l'exactitude des données par la personne concernée (le temps de la vérification).
  - le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation.
  - le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice.
  - la personne concernée s'est opposée au traitement (le temps de la vérification.)

Exemple de mesures permettant d'assurer la limitation du traitement : blocage ou déplacement des données dans un autre système empêchant leur traitement.

14. Cour de justice de l'Union européenne, arrêt de la Cour (grande chambre) du 13 mai 2014, Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González (C-131/12).

Conséquences

L'une des conséquences possibles est l'apparition de demandes d'effacement. Il est donc nécessaire d'anticiper.

- Prévoir les ressources **pour instruire les demandes dans les délais requis**.
- Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, **fixer des délais pour leur effacement ou pour un examen périodique**.
- Documenter les délais ainsi fixés dans des politiques internes **afin d'en assurer la traçabilité et l'audit.**
- **Évaluer** à chaque demande **si une disposition législative spécifique** applicable aux organismes Hlm **ne fait pas obstacle à la limitation**.
- **Vérifier la capacité** du système d'information **à gérer les limitations et leur compatibilité** avec les dispositifs de purge mis en place.
- À défaut, **mettre en œuvre des mécanismes permettant la limitation du traitement** (*systèmes d'archivage temporaire ou de verrouillage de certaines données empêchant tout traitement de la donnée pendant la durée de la limitation*).

9

ENCADRE

DROIT À L'EFFACEMENT : PRINCIPE ET EXCEPTION

Cas dans lesquels les données à caractère personnel doivent être effacées	Effacement systématique	Effacement conditionné	Dérogations de portée générale
Données ont cessé d'être nécessaires	Oui		› Limitation du traitement demandée par la personne concernée › Liberté d'expression et d'information › Obligation légale › Exécution d'une mission d'intérêt public › Motifs de santé publique › Archives, recherche scientifique ou historique ou statistiques › Constatation, exercice ou défense des droits en justice
Retrait du consentement	Non	S'il n'existe pas d'autre fondement juridique au traitement	
Données collectées auprès d'enfants	Non	- Les parents n'ont pas consenti au traitement - Exécution d'un contrat valablement conclu avec un mineur	
Opposition au traitement	Non	Le responsable de traitement ne peut pas justifier d'un motif légitime impérieux pour le traitement	
Opposition à la prospection commerciale	Oui		
Traitement illicite	Oui		
Respect d'une obligation légale	Oui		

RGPD, 65ème, 66ème 67ème et 73ème Cons., art.17, 18, 19 et 21
Repères n°1, p.11

L'ENCADREMENT PLUS RIGOUREUX DU RECOURS A LA SOUS-TRAITANCE

Le RGPD reprend les dispositions déjà contenues dans la Loi Informatique et libertés tout en précisant d'avantage les statuts et responsabilités du sous-traitant et les mesures destinées à assurer le contrôle par le responsable de traitement des opérations confiées au sous-traitant.

Principe

Le sous-traitant se voit désormais investi d'une **responsabilité propre** (en plus de celle du responsable de traitement) en ce qui concerne les mesures de sécurité à mettre en œuvre. Celle-ci n'est toutefois pas exclusive de la responsabilité de l'organisme Hlm.

- Le règlement reconnait que le sous-traitant qui **agit en dehors des instructions** du responsable de traitement **devient à son tour responsable de traitement.**
- Par ailleurs, le contenu du **contrat de sous-traitance est précisé dans le Règlement**.

Caractéristiques et contenus du contrat de sous-traitance

- **Existence d'un écrit :** nécessité d'un écrit, y compris électronique.
- **Description du traitement confié au sous-traitant :** objet et durée du traitement, Nature et finalité du traitement, Type de données à caractère personnel, catégories de personnes concernées.
- **Audit :** nécessité de prévoir l'audit des sous-traitants.
- **Notification des droits et obligations :** le contrat comporte les obligations et droits du responsable de traitement.

Conséquence

Le contrôle du recours à la sous-traitance est obligatoire pour les organismes Hlm.

- **Action sur les contrats existants :** renégocier les contrats de sous-traitance existants afin d'assurer leur conformité avec les exigences du RGPD.

Exemple : clauses-types à intégrer dans la sous-traitance de l'exploitation des données OPS.

Pour approfondir

Points de contrôle pour les organismes Hlm

- Disposer d'une politique contractuelle (modèles de contrats destinés à encadrer le recours à la sous-traitance) prévoyant que les sous-traitants ne peuvent agir que sur instruction de l'organisme, et comportant des clauses d'audit, de sécurité et de confidentialité conformes aux recommandations de la CNIL et aux exigences du RGPD.
- Conserver de manière centralisée les contrats de sous-traitance conclus.
- Disposer d'une grille d'évaluation des sous-traitants destinée à vérifier qu'ils présentent des garanties suffisantes pour assurer la mise en œuvre effective des mesures prévues (compétence, notoriété, solidité financière, lieu de localisation des serveurs ou centres informatiques, lieux d'exécution de la prestation connaissance de la législation en matière de données personnelles...).

- Assurer le contrôle effectif des mesures prévues tout au long de la durée du contrat (vérification sur documents, expertise, audits sur place...) par le prestataire et ses sous-traitants.
- S'assurer des conditions liées aux transferts de données en dehors de l'Union européenne.
- Obtenir de chaque prestataire chargé du traitement de données à caractère personnel la liste des sous-traitants de second niveau ainsi que des centres de traitement des données (y compris l'administration, la maintenance et la « hotline»)
- Documenter la réalisation d'audits auprès des prestataires et des sous-traitants de ces derniers et/ou vérifier l'existence de certifications et audits réalisés par les sous-traitants garantissant un niveau de sécurité correspondant à celui requis par la sensibilité du traitement.

- Modèle de clause à insérer dans les contrats de sous-traitance.*

RGPD, art.28
CNIL, Rapport, Les questions posées pour la protection des données personnelles par l'externalisation hors de l'UE des traitements informatiques, 9 sept. 2010[15]
CNIL, Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud, 25 juin 2012[16]

L'OBLIGATION DE RÉALISER DES ETUDES D'IMPACT SUR LA VIE PRIVEE

La réalisation d'une « étude d'impact sur la vie privée » (EIVP) est au cœur de la nouvelle méthodologie prônée par le RGPD. Elle devra être formalisée pour les traitements les plus sensibles, ainsi qu'à chaque fois que la CNIL l'aura décidé.

Principe

Une EIVP est **l'un des outils de la conformité** dont la mise en œuvre est **rendue obligatoire** pour les traitements présentant **le plus de risques** en matière de protection de la vie privée. Elle doit être conçue de telle sorte à **inclure les mécanismes** de ***« privacy by design »*** et ***« by défault ».*** Dans les cas, où elle n'est pas obligatoire, l'EIVP est un moyen d'assurer la conformité des traitements. Elle concrétise une **analyse complète des risques**, y compris des risques de violation, incluant les mesures adéquates de sécurité pour assurer la protection des données
À ce titre, La conduite d'une EIVP est une **démarche de gestion des risques** au même titre que celles mises en œuvre en matière environnementale, ou de contrôle qualité. La **CNIL** inclut progressivement dans ses **autorisations uniques** l'obligation de réaliser de telles études.

Au-delà de la démarche de conformité, l'EIVP est une démarche permettant de **gagner la confiance des parties prenantes** (personnes concernées, autorités, employés...). Ainsi, les organismes publics de l'Union européenne ou d'autres États membres rendent publiques les EIVP réalisées lorsque les traitements concernent les usagers (par exemple pour les dispositifs de vidéosurveillance).

*espace collaboratif Informatique et libertés : www.union-habitat.org
15. https://www.cnil.fr/sites/default/files/typo/document/20100909-externalisation.pdf
16. https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

La CNIL pourra également dispenser certains traitements de la réalisation d'une EIVP. Elle envisage ainsi de le faire pour tous les traitements du « Pack de conformité logement social » sous réserve que le traitement n'ait subi aucune modification au regard des exigences du pack.

- Il est possible que la CNIL fournisse tout de même un modèle d'analyse de risque à effectuer malgré l'existence des « autorisations uniques ».
- En pratique, il sera néanmoins nécessaire de garder trace des vérifications, point par point, afin de démontrer la conformité au « Pack de conformité logement social ».

Elle concrétise le passage d'une conformité formelle à une conformité effective. Il s'agit ainsi d'un processus récurrent, qui devra être renouvelé à chaque évolution majeure du traitement concerné, car la conformité doit être assurée en continu.

- Un modèle interactif d'EIVP devrait être prochainement mis en ligne sur le site de la CNIL.

Quand conduire une étude d'impact ?

En dehors des cas prévus par la loi, les circonstances qui doivent conduire à effectuer une étude d'impact sont les suivantes :

- l'introduction d'une **nouvelle technologie particulièrement intrusive :** par exemple, des capteurs RFID (Radio Frequency Identification) dans les murs des immeubles permettant des mesures de l'hydrométrie pour une optimisation des systèmes de chauffage ;
- **lorsque des traitements existants sont sujets à des changements significatifs :** par exemple, le traitement opère une nouvelle interconnexion avec d'autres bases de données pour des finalités différentes ou encore le changement d'un sous-traitant impliquant un transfert de données hors Union européenne ;
- **en cas de profilage des personnes concernées** ou croisement des données avec des informations personnelles obtenues auprès de plusieurs sources différentes afin de créer et d'établir des profils individualisé ;
- **l'introduction de nouveaux systèmes d'identification** ou l'utilisation d'identifiants conçus pour des traitements spécifiques ou réservés à des usages spécifiques: par exemple, le numéro de sécurité sociale ;
- **le suivi des individus :** la localisation ou le suivi des mouvements des personnes, y compris par caméra ;
- **augmentation significative** du nombre de données collectées ou du nombre de personnes concernées ;
- passage de la **collecte directe à la collecte indirecte**, dématérialisation de procédures ;
- **changement significatif des mécanismes de sécurité** destinés à contrôler l'accès aux données personnelles ;
- **traitements de grande ampleur** se rapportant à des **mineurs** ou des **employés** ;
- lorsqu'un traitement peut conduire à **exclure une personne du bénéfice d'un droit, d'une prestation ou d'un contrat,** alors qu'une telle exclusion n'est pas prévue par la loi ;
- ainsi que tout autre traitement listé par la CNIL.

Cas dans lesquels la conduite d'une EIVP n'est pas obligatoire

› Dispense adoptée par la CNIL.

› Traitements prévus par la loi et pour lequel le législateur a prévu une dispense (car l'EIVP a été réalisée par le législateur).

Les clarifications apportées[17] sur les notions de traitement « à grande échelle » et traitement « systématique »

› 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.

› La notion de **traitement « systématique »** renvoie aux cas suivants :
- traitement réalisé en application d'un système,
- traitement prédéfinis, organisés ou méthodiques,
- traitements réalisés en tant qu'élément d'une stratégie.

10 ENCADRE

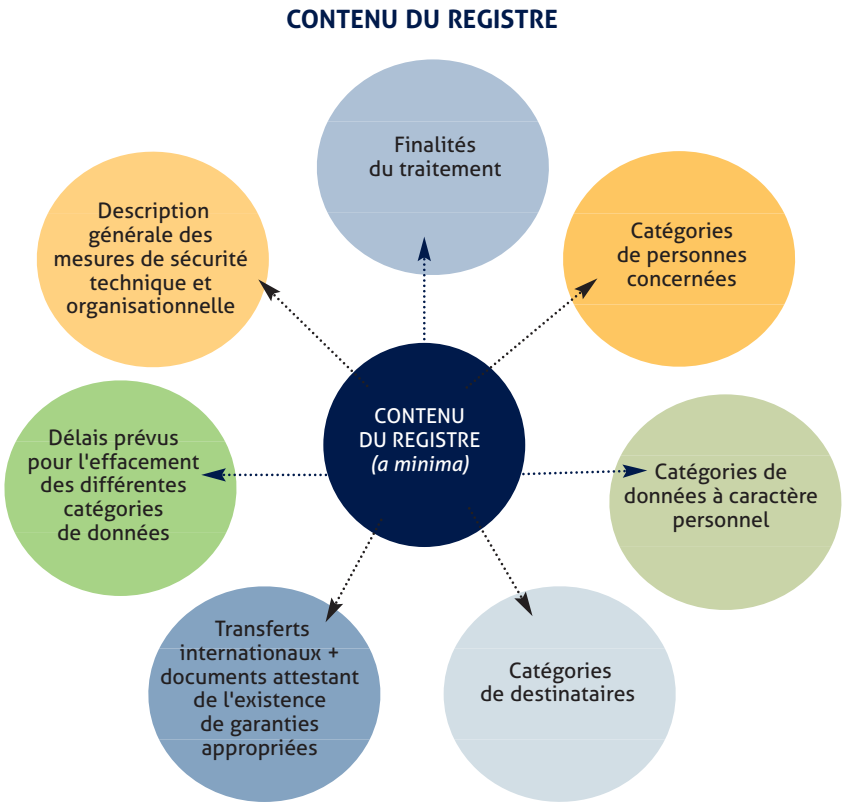
LES DIFFÉRENTES ÉTAPES D'UNE EIVP ET LES IMPACTS POUR LES ORGANISMES HLM*

› La conduite d'une EIVP constitue une démarche projet à part entière comportant plusieurs étapes	Cf. partie 5
› Vérification documentée du bon respect des éléments du « Pack de conformité logement social »	Cf. Repères n°1
› Identification des autres traitements à risques Formalisation de l'analyse des risques	
› Programmation de la réalisation des EIVP	Cf. partie 5

17. G29, WP 243 et 248, Lignes directrices relative au DPO et relatives à la conduite d'une EIVP.
* Cf. Partie 5, la démarche d' « accountability » en pratique.

LE REGISTRE DES TRAITEMENTS : OBLIGATOIRE, DÉCONNECTÉ DU DPO ET REVISITÉ DANS SON CONTENU

Chaque organisme Hlm doit tenir un registre de l'ensemble des traitements qu'il met en œuvre. Cette obligation* concerne également les sous-traitants pour les traitements mis en œuvre pour le compte de leurs clients.



Principe

Le RGDP ne prévoit pas que le registre soit accessible à toute personne en faisant la demande. Il n'est toutefois pas exclu que la loi française maintienne cette exigence.

Conséquences

Le registre doit être complet pour l'entrée en application du règlement. Aucun délai supplémentaire n'étant prévu par le règlement, des mesures doivent donc être prises par les organismes Hlm :

- **Étape préalable indispensable** : l'état des lieux et le recensement des traitements.**
- **Alimentation du registre pour les organismes disposant d'un CIL :** compléter le registre avec les traitements dispensés de formalités ou relevant d'un régime d'autorisation si le registre est incomplet.
- **Traitements visés dans le pack de conformité :** la seule référence au pack n'est pas suffisante. Chaque traitement doit être recensé avec un niveau de granularité suffisant pour que la description permette de comprendre l'étendue du traitement ; il ne paraît en effet plus possible de se référer aux normes du « Pack de conformité logement social » qui sont génériques, alors que la description figurant au registre est spécifique.

* Mise à jour fiche d'identification du traitement : Repères n°1, p.31, espace collaboratif Informatique et libertés, www.union-habitat.org
** Cf. Repères n°1 p.24

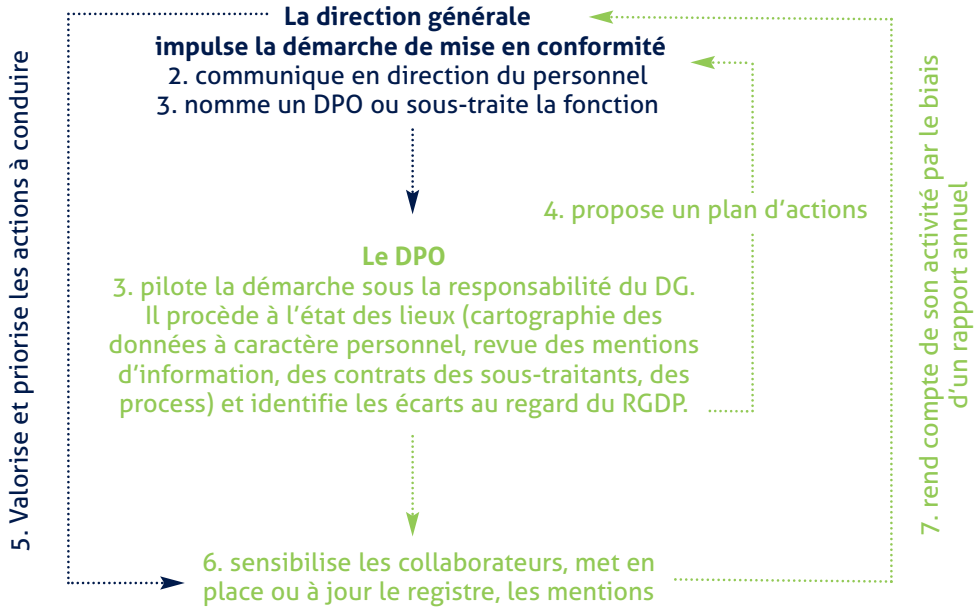
PARTIE 5

La démarche d'« accountability » en pratique

ETAPE 1
CONSOLIDER LA DÉMARCHE DE CONFORMITÉ

Élément n°1 : METTRE EN PLACE LA GOUVERNANCE

La mobilisation de l'ensemble des services doit se poursuivre et la direction générale des organismes doit être pleinement investie. Elle doit impulser la démarche, l'organiser et conduire les arbitrages nécessaires le cas échéant. **Le rôle des directions générales est d'autant plus affirmé qu'on observe une croissance importante des risques pour les organismes Hlm.**



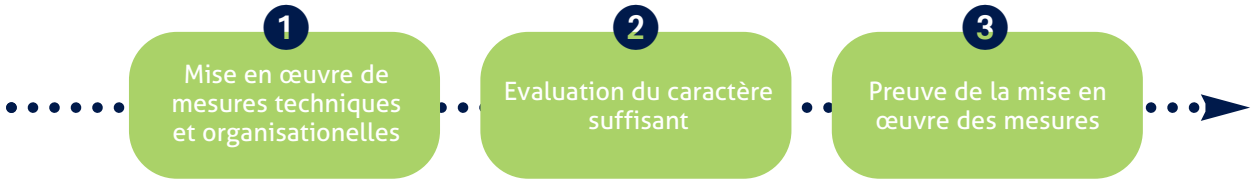
La sensibilisation des équipes dirigeantes et du personnel des organismes est plus que jamais une priorité. La gouvernance devra être formalisée et renforcée afin d'assurer l'effectivité de l'application du RGPD. Les organismes Hlm doivent donc poursuivre la mobilisation des équipes pour assurer la mise en œuvre des actions de conformité déjà identifiées dans le Cahier Repères n°1.

Les principes et modalités d'analyse restent identiques et la démarche d'« accountability » s'inscrit dans la continuité. L'effet de l'entrée en application du RGPD consiste à **généraliser l'approche déjà envisagée par la CNIL en 2014 dans son label gouvernance**[18].

› Elle impose un formalisme plus poussé et une **exigence d'efficacité et d'effectivité** des mesures déjà prises pour se conformer à la loi Informatique et libertés.

18. Délibération n° 2014-500 du 11 décembre 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de procédures de gouvernance Informatique et libertés

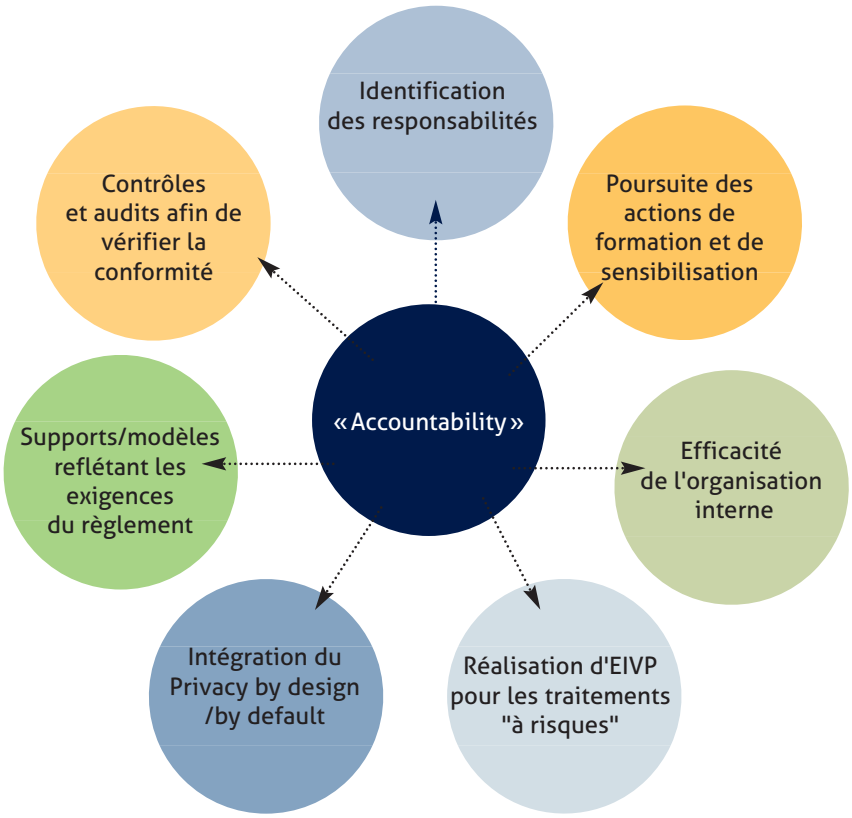
› Elle s'inscrit dans un **cycle destiné à assurer la conformité continue** des traitements de données à caractère personnel selon trois axes principaux :



› L'application du RGPD s'apparente à la mise en place d'un « écosystème de la donnée » visant à garantir la confidentialité et la sécurité des données **en ayant en perspective les risques générés par les traitements pour les personnes concernées**.

11 ENCADRE

RESPECTER LE PRINCIPE DE RESPONSABILITÉ



La complexité de la réglementation et les marges d'interprétation imposent d'effectuer une veille régulière sur les avis, recommandations émis par la CNIL et le Comité européen de la protection des données qui va succéder au G29.

TEMOIGNAGE

Marc ZUMBRUNNEN, responsable audit et conformité, CIL VALOPHIS HABITAT* depuis 2012

La mise en place du RGPD

L'arrivée du RGPD n'est pas une révolution au regard des principes. **Il y a incontestablement un changement d'approche** (approche par les risques) qui impose d'être en mesure de rendre compte d'une documentation complète sur la conformité des traitements, et rend essentielle la coordination avec toutes les entités au sein de l'OPH.

Premières actions et réalisations

- Important travail d'appropriation de la règlementation
- Tour de l'ensemble des directions pour à la fois sensibiliser et obtenir une connaissance des traitements
- Recensement des traitements
- Améliorer la gouvernance pour la rendre plus proactive
- Actions de sensibilisation sur l'arrivée du RGPD en janvier 2017, à renouveler en 2018
- Mise en place d'une procédure de notification de violations de données à caractère personnel
- Mise en place d'un plan d'action à déployer jusqu'en mai 2018

Méthodologie déployée

- Mettre en place une gouvernance avec la participation du juridique et du responsable de la sécurité des systèmes d'information
- Sensibiliser les agences de proximité afin de permettre l'acquisition de réflexes
- Rédaction de procédures sur le droit d'accès, le contrôle CNIL et la gestion des habilitations.

Conseils aux futurs DPO

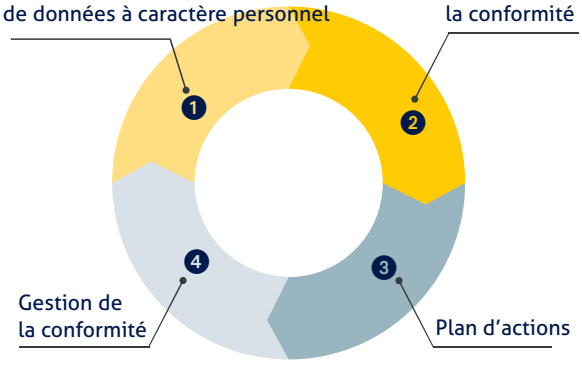
- Décortiquer et analyser le RGPD en incluant les considérants afin de se l'approprier
- Faire le tour de toutes les directions
- Diagnostiquer l'état de l'organisme et des différents services, puis se positionner sur les évolutions et les améliorations
- Effectuer des priorisations.

* OPH, 36 458 logements (44 127 niveau groupe), 945 salariés

Élément n°2 : RÉALISER UN DIAGNOSTIC ET RÉDIGER UNE FEUILLE DE ROUTE*

1 Identifier et décrire des traitements (*automatisés ou non*) de données à caractère personnel

Accomplir les formalités CNIL le cas échéant



2 Analyse de conformité à la loi Informatique et libertés et au RGPD pour chacun des traitements

Sensibilisation des responsables de traitements

3 Définition et mise en place des actions de mise en conformité par rapport aux obligations de la loi et du RGPD

4 Assurer la conformité dans la durée, avec la maintenance des formalités et la diffusion d'une culture informatique et libertés

L'analyse de conformité

1. Collecter et traiter des données proportionnées (nécessaires) au regard de la finalité du traitement
2. Droit d'accès et d'information des personnes concernées
3. Assurer la confidentialité des données collectées
4. Assurer la sécurité des données collectées
5. Conserver les données pour une durée limitée

Les points à traiter en priorité

- Encadrer la collecte et le traitement des données sensibles
- Contrôle et vérification des zones de textes libres
- Encadrer la transmission de données à des tiers
- Définir une politique des habilitations et veiller à leur mise à jour
- Mettre les systèmes d'information en conformité avec les exigences CNIL
- Définir des durées de conservation des données dans les bases actives et limiter les accès aux archives
- Encadrer l'usage de la vidéosurveillance ou vidéoprotection
- Sécuriser les traitements relatifs à la tranquilité et la sécurité résidentielles
- Organiser l'exercice du droit d'accès des personnes aux données qui les concernent
- Traiter les dossiers à caractère personnel

* Cartographie des processus métiers, exemple de liste des traitements d'un organisme, grille d'état des lieux, modèle de fiche de traitement disponibles sur l'espace collaboratif Informatique et libertés : www.union-habitat.org

TÉMOIGNAGE

Jean-Yves THOMAS, responsable des affaires générales, CIL partiel mutualisé, Réseau BATIGÈRE

La mise en place du RGPD

Comme une chance et non une nouvelle contrainte de nouveaux textes règlementaires imposant de nouveaux bouleversements dans l'approche Informatique et Libertés.
Les dispositions de la loi Informatique et Libertés, le pack de conformité « bailleurs sociaux » ne vont pas disparaitre. Les grands fondements resteront dans le RGPD. Des ajustements seront néanmoins nécessaires. La responsabilité est accrue sur les entreprises, les contraintes administratives de déclaration seront moins fortes. Pour autant, il convient de se préparer dès maintenant pour mettre en place une organisation permettant d'optimiser les règles de contrôle et d'audit interne et de documenter davantage, mieux formaliser les décisions, process, etc.

Premières actions et réalisations

- Rencontrer l'ensemble des directeurs généraux afin de promouvoir la démarche de conformité et l'intérêt de nommer un CIL
- Organisation administrative de la fonction (dont le recensement des traitements)
- Poursuite et actualisation des actions de formation
- Élaboration de lignes directrices sur la tenue de la documentation
- Redéfinition de l'organisation et du périmètre des fonctions du CIL et des RILs (référents informatique et libertés)

Méthodologie déployée

- Nomination des relais informatiques et libertés (RIL) dans toutes les filiales
- Création d'un intranet dédié.
- Mise en place d'un module de formation avec l'aide d'un organisme spécialisé de 4h pour le personnel (du gardien à la direction générale) : en 3 ans près de 700 personnes ont déjà bénéficié de cette formation.
- Mise en place d'une charte « Informatique et libertés ».

Conseils aux futurs DPO

- Faire une lecture précise du RGPD et de ressortir les points majeurs qui modifient l'approche informatique et libertés dans nos organisations par rapport à la réglementation en vigueur (loi Informatique et Libertés, norme NS20, pack de conformité).
- Pour ce qui me concerne, je pense communiquer largement en interne et en particulier auprès des organes de direction (CODIR, réunions de services, etc.), et en particulier auprès des responsables de traitement à compter de septembre 2017. Je pense réaliser un document synthétique présentant les points forts du RGPD et les actions à mettre en œuvre pour une application à compter de mai 2018. J'ajouterai à ces actions les acteurs internes qui seront concernés par ces nouvelles dispositions, notamment les Relais Informatique et Libertés présents dans nos différentes structures.

* ESH, 155 000 logements, 1 700 collaborateurs (UES BATIGERE)

12

ENCADRE

LE RÔLE DES DIFFÉRENTS ACTEURS DANS LA DÉMARCHE DE CONFORMITÉ

Tout comme pour le CIL (*cf. Repères n°1, p.14*), la désignation d'un DPO ne dispense pas la direction générale des organismes Hlm de leur responsabilité dans la mise en œuvre des traitements de données à caractère personnel et en particulier de leurs obligations de définir un cadre organisationnel et procédural approprié afin d'assurer la conformité des traitements.

Le DPO ne peut agir seul et son action doit s'inscrire dans une gouvernance impliquant tous les acteurs de la conformité au sein de l'organisme Hlm.

La direction générale

- Elle est reponsable de la démarche de conformité dans son ensemble
- Elle définit la politique et des règles générales en matière de protection des données à caractère personnel, les rôles et fonctions des métiers chargés de la protection des données et arbitre également les difficultés rencontrées lors de la mise en oeuvre des traitements
- Elle définit et contrôle le repect de la politique de sécurité des systèmes d'information (PSSI)
- Elle endosse juridiquement la qualité de responsable de traitement
- Elle organise le contrôle du respect des règles informatiques et libertés
- Elle s'assure de la mise en oeuvre de la démarche de conformité par les responsables opérationnels qu'elle a désignée pour agir par délégation en son nom
- Elle veille à garantir le le statut du DPO (s'assurer de son indépendance fonctionelle, allouer les moyens humains, assurer sa formation)

Autres fonctions support (audit, conformité, RSE...)

- Assistance des directions opérationnelles
- Soutien actif de la direction sur toutes les problématiques de conformité

Les direction opérationnelles /chef de projet (direction métier)

- Les directions opérationelles sont responsables de tout ce qui concerne la mise en oeuvre des mesures ainsi que de la détermination des moyens de traitements de données à caractère personnel dans le repect de l'impulsion donnée par la direction générale : définition des finalités, des moyens, recours à la sous-traitance...
- Elles expriment les besoins de sécurité et de minimisation des données dans le respect de la PSSI
- Elles recueillent les visas/avis des différentes parties prenantes (DPO, filière sécurité, juridique, audit...)
- Elles réalisent les analyses de risque pour le compte de la direction générale et le cas échéant font valider les risques résiduels par la direction générale

Le DPO

- En sa qualité d'expert, il est consulté lors de la mise en oeuvre ou de la modification de nouveaux systèmes et traitements informatiques
- Il a un rôle essentiel de conseil pour tout ce qui concerne la mise en oeuvre de mesures comme la détermination de moyens assurant le traitement des données personnels et leur sécurtié (utilisation des moyens tels que le privacy by design, recours à la sous-traitance, ou mise en oeuvre d'EIVP, et d'audits).
- Il contrôle le respect des obligations légales et règlementaires, la mise en oeuvre de mesures de "privacy by design" ainsi que la mise en oeuvre des conseils et recommandations relatifs à la gestion des traitements et à leur sécurité.
- Pour les traitements comportant des risques particuliers, le DPO alerte la direction générale sur les difficultés rencontrées
- Il peut se voir attribuer par la direction générale un rôle de coordinateur des aspects règlementaires liés au traitement de données à caractère personnel

Filière sécurité/ DSI

- Rôle de conseil sur le choix des technologies et les mesures de sécurité à adopter ainsi que dans la sélection des sous-traitants
- Garant de la sécurité des systèmes d'informations
- Conduite de l'analyse des risques liés à la sécurité des traitements
- Audit des sous-traitants
- Assimilation et intègration des nouvelles technologies

ETAPE 2
ADAPTER LES MESURES MISES EN ŒUVRE DANS LE CADRE DU PACK DE CONFORMITÉ

Élément n°1 : NOMMER UN DPO

La gestion de la conformité passe par la mise en œuvre de mesures organisationnelles et techniques destinées à maintenir la conformité dans la durée et prévenir les manquements futurs. Celles-ci complètent celles déjà envisagées dans le Cahier Repères n°1.

La désignation d'un pilote est une étape indispensable : le DPO a vocation à être ce pilote.

Il doit pouvoir s'appuyer à la fois sur
- les relais internes (RIL) précédemment désignés selon la taille de l'organisme Hlm
- des experts internes (juridiques, sécurité informatique, opérationnels), voire externes
- un circuit de validation interne destiné à recueillir les avis des experts et obtenir la validation opérationnelle des décisions se rapportant aux traitements.

Ce circuit de validation est propre à chaque organismes Hlm : il dépend de sa taille, de sa structure et des processus décisionnels existants. Il s'agit d'établir une organisation adaptée à l'organisation existante pour que les aspects « loi Informatique et libertés » soient intégrés aux différentes phases de la mise en œuvre d'un traitement :
- Étude de faisabilité
- Choix de la solution/conception
- Contractualisation avec le prestataire
- Réalisation et test, mise en œuvre/déploiement
- Guides pour les utilisateurs
- Information des personnes concernées
- Évolutions

Le DPO doit être impliqué aux différentes étapes de la réalisation d'un projet informatique et doit pouvoir s'appuyer sur les experts internes ou externes

L'action du CIL/DPO doit pouvoir être relayée par :
- l'intégration dans les processus métiers de « points de conformité CNIL » à vérifier (minimisation des données, durée de conservation à appliquer, règles d'archivage, recours au chiffrement...),
- la mise en place de modèles (clauses contractuelles, notices d'information, réponse aux demandes de droit d'accès, annexe sécurité des contrats de prestation informatique, fiche de sécurité pour chaque projet...) rédigés par les experts (juridiques et informatique) en concertation avec le DPO,
- des actions de sensibilisation régulières à la loi Informatique et libertés,
- la diffusion des règles de sécurité utilisateurs et des mesures de sécurité à appliquer sur les systèmes et applications informatiques.

Repères n°1, p. 27-28, 54 et 58

Élément n°2 : DÉFINIR UN PLAN D'ACTIONS

La méthodologie diffère peu de la démarche de mise en conformité présentée dans le Cahier Repères n°1. **Ceci montre que les actions à engager dans le cadre du processus de mise en conformité au regard du RGPD s'inscriront nécessairement dans la continuité du plan d'action initialement mis en place à la suite de la publication du « Pack logement social ».**

Comme dans la première phase de mise en conformité, les différentes étapes doivent être engagées de manière itérative, en fonction des sujets les plus sensibles à traiter en priorité et de l'état d'avancement de chacun des organismes.

Domaine 1 – Recensement/connaissance des traitements

Action n°1	Poursuivre l'état des lieux	Repères n°1, étape n°1
Action n°2	Identification de la responsabilité sur les traitements	Encadré n°2 Encadré n°3
Action n°3	Identification de la base légale des traitements	Encadré n°6
Action n°4	Constitution/mise à jour du registre	Partie 4, page 52 Partie 5, page 66 Encadré n°17
Action n°5	Tenue de la documentation/cartographie des traitements	Partie 5, élément n°4 Encadré n°6 Encadré n°18

Domaine 2 - Formation / sensibilisation des personnels

Action n°6	Action n°6 Poursuivre la formation et sensibilisation des personnels en intégrant notamment l'évaluation des risques et la tenue de la documentation relative aux traitements	Repères n°1, actions 17, 18, 22, 27
Action n°7	Identification de la responsabilité sur les traitements	Partie 4, pages 35 à 40

Domaine 3 - Renforcer la gouvernance sur les traitements

Action n°8	Désignation du DPO et le cas échéant des relais Informatique et Libertés	Repères n°1, étape préalable + étape 4
Action n°9	Identifier les responsabilités et les circuits de signature	Repères n°1, pages 27-28 Étape 2 (3) Encadré n°16 Fiche pratique n°4
Action n°10	Rédiger les procédures complémentaires	Repères n°1, page 40 Encadré n°15

Domaine 4 – Procédures

Action n°11	Faire la revue des procédures existantes	Encadré n°15
Action n°12	S'assurer de l'efficacité des procédures destinées à assurer l'effectivité des droits d'accès et rectification des personnes concernées	Partie 3, page 34
Action n°13	Respect des règles relatives aux durées de conservation	Partie 4, pages 46 et 47
Action n°14	Revoir les règles de gestion du système d'information	Encadré n°19 Encadré n°20 Encadré n°22

Domaine 5 – Documentation contractuelle

Action n°15	Revue des contrats de sous-traitance et des conventions avec les tiers	Partie 4, page 48 Encadré n°19
Action n°16	Revue de la documentation des droits et habilitations, de la politique d'archivage	Repères n°1
Action n°17	Programmation de la réalisation des EIVP	Partie 4, pages 49 à 51
Action n°18	Révision des modèles de clauses/mentions d'informations/clauses de recueil de consentement	Encadré n°4 Fiche pratique n°3

Domaine 6 – Conduite des études d'impact

Action n°19	Vérification documentée du bon respect des éléments du « Pack de conformité logement social »	Repères n°1
Action n°20	Identification des autres traitements « à risques » Formalisation de l'analyse des risques	Encadré n°21
Action n°21	Programmation de la réalisation des EIVP	Élément 5, page 70

Domaine 7 – Vérifications et contrôles

Action n°22	Conduite d'audits /Vérifications des audits réalisés par les sous-traitants	Partie 5, page 71
Action n°23	Efficacité de la procédure de détection des violations de données	Partie 5, page 71

Élément n°3 : ÉVALUER LE CARACTÈRE SUFFISANT DES MESURES (APPROCHE PAR LES RISQUES)

L'identification des risques

Pour apprécier le caractère suffisant des techniques ou organisationnelles à mettre en œuvre au regard des risques présentés par le traitement, le RGPD donne de nombreux exemples des risques à considérer :

- traitements susceptibles d'entraîner des dommages physiques, matériels ou moraux,
- traitements pouvant engendrer des discriminations,
- traitement pouvant faciliter ou exposer la personne à un vol ou à une usurpation d'identité, à une perte financière, à une atteinte à la réputation, à une perte de confidentialité de données protégées par le secret professionnel, lorsqu'il s'agit d'un traitement des données sensibles, lorsque des aspects personnels sont évalués, etc.

Exemple : la collecte et la conservation des RIB des locataires doivent faire l'objet d'une attention particulière du fait des risques de préjudices financiers en cas de détournement de ces données.

Autres critères pouvant être pris en compte :

- Sensibilité des données
- Nombre de personnes concernées
- Qualité des personnes concernées (VIP, mineurs...)
- Nombre de personnes pouvant accéder au traitement
- Durée de conservation des données
- Quantité de données à caractère personnel traitées
- Recours ou non à la pseudonymisation
- Nombre destinataires / diffusion incontrôlée
- Modalités de transmission
- Caractère intrusif / technologie utilisée
- Risque de détournement de finalité
- Interconnexions / échanges de données
- Exactitude/mise à jour des données

Les traitements pré-qualifiés comme « à risques » dans le RGPD

- ayant pour objet le profilage des personnes utilisé pour la prise de décisions à l'égard des intéressés ou les affectant de manière significative (*réalisés « à grande échelle » et de manière « systématique »*),
- la vidéosurveillance « à grande échelle[19] »,
- portant sur les catégories particulières de données (*par exemple, données de santé ou des difficultés sociales*), dont les données **biométriques** (*par exemple, collaborateurs des bailleurs qui utilisent leurs empreintes digitales pour accéder à leur système d'information*),
- portant sur des données relatives aux mineurs,
- identifiés comme présentant des risques particuliers pour les personnes (rôle de l'EIVP),
- qui seront listés par la CNIL en vue de l'entrée en application du RGPD ou ultérieurement.

RGDP, Cons. 75 et 76 - CNIL, guides EIVP
PIA-1, la méthode : comment mener une EIVP ?
PIA-2, l'outillage : modèles et bases de connaissances de EIVP
PIA-3, les bonnes pratiques : mesures pour traiter les risques sur les libertés et la vie privée
G29, lignes directrices sur les EIVP (en anglais), wp. 248

19. Terme qui reste encore imprécis : dans le cas où il existerait une incertitude, il reste préconisé d'effectuer une EIVP

ETAPE 3
DOCUMENTER LA DÉMARCHE

Les organismes Hlm devront pouvoir démontrer la conformité des traitement de données avec le RGPD. Cette obligation porte non seulement sur l'existence des mesures mais également sur leur efficacité au regard des risques identifiés.

Plusieurs outils sont envisagés par le RGPD pour leur permettre d'apporter **la preuve de la conformité** des traitements :

- **Élément n°1** : une organisation interne appropriée
- **Élément n°2** : des procédures pour ancrer la démarche de conformité dans les processus métiers
- **Élément n°3** : la formalisation de la documentation relative aux traitements (cartographie)
- **Élément n°4** : la tenue du registre des traitements
- **Élément n°5** : la revue des règles de gestion du système d'information

Élément n°1 : UNE ORGANISATION INTERNE APPROPRIÉE

La mise en œuvre de la démarche de conformité nécessite, pour les directions générales des organismes Hlm, d'identifier :

- une matrice des responsabilités et d'un circuit de validation **(élément n°1.1)**
- un mécanisme de coordination entre les différents services concernés par la mise en œuvre des traitements : CIL/DPO, Informatique, DSI, responsable sécurité des systèmes informatiques-RSSI, juridique, RH, marketing, audit, risque... **(élément n°1.2)**
- des moyens, notamment humains et budgétaires, nécessaires pour assurer l'efficacité de la démarche **(élément n°1.3)**

Repères n°1 p.27-28
Encadré n°16 : le rôle des différents acteurs

Élément n°2 : DES PROCÉDURES POUR ANCRER LA DÉMARCHE DE CONFORMITÉ DANS LES PROCESSUS MÉTIERS

La rédaction de politiques internes, notes et programmes de formation, destinés à assurer de manière concrète et opérationnelle, **le respect de la législation** en matière de protection des données personnelles **par les personnels et sous-traitants,** incombe à la direction générale des organismes Hlm.

13 ENCADRE

LES PROCÉDURES À DOCUMENTER OU À METTRE À JOUR PAR LA DIRECTION GÉNÉRALE

Nouvelles procédures	
2.1 Note stratégique concernant le pilotage de la démarche de mise en conformité, qui définira le mode de gouvernance, les moyens affectés et le plan d'actions...	
2.2 Organisation et responsabilités (DPO, matrice des responsabilités (RACI)/ circuits de visas)	Fiche pratique n°3, page 84 : exemple de RACI
2.3 Procédure sur l'analyse des risques et la réalisation des EIVP.	
2.4 Procédure sur les violations de données à caractère personnel	Élément n°5/5.5
Procédures à mettre à jour (le cas échéant)	
2.5 Procédure sur le respect des droits des personnes, le traitement des demandes d'accès des personnes	
2.6 Politique de durée de conservation et archivage	www.club-ebios.org/site/productions.html
2.7 Politiques de sécurité, de gestion des habilitations	Repères n° 1 page 64, actions 15 et16
2.8 Procédure sur la relation avec l'autorité de contrôle, notamment conduite à tenir en cas de contrôle*	espace collaboratif Informatique et libertés : processus de gestion de crise. www.union-habitat.org

* Mise à jour de la fiche d'identification de traitement : espace collaboratif informatique et libertés. www.union-habitat.org

Elément n°3 : LA FORMALISATION DE LA DOCUMENTATION RELATIVE AUX TRAITEMENTS (CARTOGRAPHIE)

Plusieurs éléments devront faire l'objet d'une documentation (*i.e. traçabilité écrite*) dont la tenue devra être auditée. Elle constituera un gage du respect du RGDP et de la bonne mise en œuvre de la démarche de conformité par les organismes Hlm.

L'intérêt de la tenue d'une telle documentation n'est pas nouvelle dans son principe car elle répondait déjà à la méthodologie à adopter afin d'assurer le respect de la législation. Elle est déjà prise en compte par la CNIL dans le cadre des vérifications (contrôles) qu'elle opère.

Elément n°4 : La tenue du registre des traitements

La tenue du registre des traitements devient obligatoire. Ce registre comporte des éléments nouveaux qui ne figuraient pas dans celui du CIL.

14 ENCADRE

LE CONTENU DU REGISTRE DES TRAITEMENTS

Éléments déjà contenus dans le registre du CIL (cf. Repères n°1, p 31)	Éléments complémentaires qui devront figurer au registre des organismes Hlm
› Nom et coordonnées du responsable de traitement	› Noms et coordonnées du responsable conjoint du traitement
› Finalités du traitement	› Nom et coordonnées du DPO
› Service chargé de la mise en œuvre	› Transferts internationaux + documents attestant de l'existence de garanties appropriées
› Fonction de la personne ou le service auprès duquel s'exercent les droits des personnes ainsi que leurs coordonnées	› Les délais prévus pour l'effacement des différentes catégories de données
› Catégories de personnes concernées	› Une description générale des mesures de sécurité techniques et organisationnelles
› Catégories de données à caractère personnel	
› Catégories de destinataires	
› Durée de conservation des données	
› Date et objet des 3 dernières mises à jour	

* Mise à jour de la fiche d'identification de traitement : espace collaboratif informatique et libertés. www.union-habitat.org

15

ENCADRE

LA DOCUMENTATION À TENIR POUR CHAQUE TRAITEMENT

Les éléments de connaissance détaillée du traitement

- Les systèmes de traitements de données à caractère personnel,
- Le recours à des prestataires externes dans le cadre du traitement de données à caractère personnel
- Les flux de données à caractère personnel (interfaçages, flux externes)
- L'existence ou non d'un transfert hors Union européenne et, le cas échéant, la finalité du transfert, les catégories de personnes concernées, la nature des données transférées, les catégories de destinataires du transfert (filiale, prestataire, etc.), la nature des traitements opérés chez le destinataire, le pays d'établissement et la garantie permettant d'encadrer le transfert (telle que les BCR, clauses contractuelles types et Privacy Shield)
- L'existence ou non de la sous-traitance d'une activité de traitement de données à caractère personnel (avec mention de l'existence et de la date de signature du contrat de sous-traitance comportant une clause Informatique et libertés) ;
- Un niveau de vraisemblance et de gravité pour l'ensemble des risques liés au traitement
- Pour les sites internet : les éléments de sécurité, l'utilisation de cookies

Analyse de conformité comprenant a minima :

- Identification du fondement légal du traitement
- L'évaluation de la pertinence et de la nécessité du traitement et du recours à des données à caractère personnel
- Modalités et contenu de la notice d'information des personnes, des clauses et modalités de recueil du consentement
- La revue des contrats de sous-traitance de données à caractère personnel

Politique de conservation et d'archivage appliquée :

- Description des modalités de conservation et de destruction ou archivage des données

Analyse des risques et mesures de sécurité mises en œuvre :

- Évaluation des risques liés au traitement pour les personnes concernées
- Description des politiques et mesures de sécurité applicables au traitement

Respect du circuit de validation :

- Avis, visas et validation obtenus

Accomplissement des formalités (si applicable) :

- Preuve de la réalisation des EIVP
- Preuve de l'accomplissement des formalités CNIL (consultations préalables de la CNIL)

Contrôle et vérifications réalisées :

- Vérifications lors du recours à la sous-traitance
- Audits réalisés

Une **cartographie** qui liste l'ensemble des traitements d'un organisme en fonction de leur finalité, est réalisée à partir de l'état des lieux *(cf. Repères n°1 p.29)*. Elle doit être actualisée régulièrement : il s'agit d'identifier *(par exemple, à partir de la liste article 31 des déclarations effectuées auprès de la CNIL ou du registre tenu par le CIL),* l'ensemble de traitements ou systèmes de traitements mis en œuvre. Elle dépasse le cadre des informations obligatoires à la tenue du registre du CIL, car elle constitue une vision globale sur les traitements permettant de démontrer la conformité et elle identifie les flux de données.

Elément n°5 : LA REVUE DES RÈGLES DE GESTION DU SYSTÈME D'INFORMATION

5.1 Le recours à la sous-traitance

Des vérifications de conformité sont à effectuer par la DSI en cas de recours à la sous-traitance à la fois lors de la sélection, de la contractualisation et de l'exécution de la prestation sous-traitée.

16 ENCADRE

VÉRIFICATIONS À EFFECTUER EN CAS DE RECOURS À LA SOUS-TRAITANCE

Phase concernée	Vérifications à opérer
Sélection	**Vérifier** que le sous-traitant présente des garanties suffisantes pour assurer la mise en œuvre effective des mesures prévues (compétence, notoriété, solidité financière, lieu de localisation des serveurs ou centres informatiques, lieux d'exécution de la prestation, connaissance de la législation en matière de données personnelles...) **S'informer** de la liste des sous-traitants et les pays d'exécution de la prestation, afin d'anticiper sur l'application des règles spécifiques liées au transfert de données en dehors de l'Union Européenne, et, tout au long du contrat.
Contractualisation	**S'assurer** du respect de la politique contractuelle définie par l'organisme Hlm notamment en matière de sécurité et protection des données à caractère personnel. **Faire renseigner** par le prestataire un plan d'assurance sécurité (PAS).
Exécution	**Assurer** le contrôle effectif des mesures prévues permettant d'en vérifier le respect (vérification sur documents, expertise, audits sur place...) par le prestataire et ses sous-traitants.

5.2 Le recours à la sous-traitance

Afin de pouvoir démontrer la conformité des traitements aux exigences du RGPD, la DSI doit pouvoir justifier des éléments de mesures organisationnelles et techniques destinées à démontrer la prise en compte des exigences de sécurité.

17 ENCADRE

MESURES ORGANISATIONNELLES ET TECHNIQUES DESTINÉES À DÉMONTRER LA PRISE EN COMPTE DES EXIGENCES DE SÉCURITÉ

Mesures organisationnelles destinées à démontrer la prise en compte des exigences de sécurité

- Documenter la sécurité pour chaque application/système informatique.
- Documenter l'analyse de risques pour l'ensemble des traitements comportant des données à caractère personnel.
- Pour chaque traitement ou système de traitement, tenir le schéma des flux (au besoin processus par processus).
- Définir une politique de sécurité adaptée aux risques présentés par les traitements et à la taille de l'organisme (cette politique devant décrire les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre).
- Définir une politique d'accès et d'habilitation limitant l'accès aux données à caractère personnel identifiées aux seules personnes autorisées sur la base du principe du « *besoin d'en connaître* » au regard de leurs fonctions.
- Assurer la formation et la sensibilisation des utilisateurs aux règles de sécurité.
- Tenue du registre des violations de sécurité.
- Tenue du registre des demandes d'effacement et de limitation du traitement.

Mesures techniques destinées à démontrer la prise en compte des exigences de sécurité

- Assurer que les données à caractère personnel ne sont traitées que si la finalité du traitement ne peut être raisonnablement atteinte par d'autres moyens.
- Conduire des analyses de risques afin d'identifier les mesures de sécurité appropriées.
- Règles relatives aux droits d'accès et aux habilitations (les droits permettant d'accéder aux données devant être précisément définis en fonction des besoins réels de chaque utilisateur, il s'en suit que les permissions d'accès doivent être supprimées pour tout utilisateur n'étant plus habilité).
- Conditions d'administration et de maintenance du système d'information prévoyant l'existence de systèmes automatiques de traçabilité (journaux, pistes d'audits, interventions de maintenance, profils différenciés selon les rôles...).
- Justificatif de l'effacement des données, destruction de supports de stockage, nettoyage du matériel remisé de toute donnée à caractère personnel.

5.3 La conduite et la documentation des analyses de risques

La conduite et la documentation des analyses de risques relève de la responsabilité de la direction des systèmes d'information, avec l'assistance le cas échant du DPO et d'experts externes.

Le risque devrait faire l'objet d'une **évaluation objective** permettant de déterminer si les opérations de traitement des données comportent un risque élevé. Il convient dans ce cas de déterminer le risque en termes de probabilité et de gravité, en fonction de la nature, de la portée, du contexte et des finalités du traitement de données.

Selon le RGDP (considérant 60 ter), il faut interpréter la notion de risque élevé comme **un risque particulier** de porter atteinte aux droits et aux libertés des personnes physiques.

La CNIL a détaillé dans ses guides relatifs aux EIVP la méthodologie de la démarche d'analyse des risques à partir d'une simplification de la méthodologie EBIOS. Elle travaille actuellement sur la simplification de cette méthode et devra fournir un modèle interactif de réalisation d'EIVP.

Cette méthodologie n'est toutefois pas la seule permettant d'effectuer une analyse de risques et l'organisme Hlm devra identifier celle qui est la plus adaptée à sa taille et sa structure, ainsi qu'à la complexité de ses systèmes d'information. Pour identifier la méthode adaptée, le recours à un expert externe peut parfois s'avérer utile.

COMMENTAIRE

Pour que les organismes Hlm soient à même d'inclure la démarche d'analyse des risques dans les process opérationnels, **il est nécessaire de former les DSI.** La démarche d'analyse des risques et les outils nécessaires pour la conduire vont se construire en interne progressivement.

CNIL guides
PIA-1, la méthode : comment mener une EIVP
PIA-2, l'outillage : modèles et bases de connaissances de l'EIVP
PIA-3, les bonnes pratiques : mesures pour traiter les risques sur les libertés et la vie privée
ISO/IEC 29134 (Privacy Impact Assessment–Methodology)

Où trouver des exemples d'analyse des risques ?
- AU-053, Contrôle d'accès biométrique avec base centrale, grille d'analyse des risques
- Club E-BIOS, https://www.club-ebios.org/site/productions.html :
- Gestion des patients dans un cabinet de médecine du travail - Étude de cas (29/11/2011)
- Géolocalisation de véhicules d'entreprise - Étude de cas (17/03/2017)
- GS1 EPC/RFID Privacy Impact Assessment Tool : Protecting consumer's personal data in RFID implementations : https://www.gs1.org/pia

5.4 La réalisation de controles et certifications

L'obligation de démontrer la conformité des traitements impose également d'assurer le contrôle et la vérification de l'efficacité de l'organisation et des règles tout au long de leur mise en œuvre.

En plus des éléments classiques relatifs à la sécurité du SI, disponibilité, intégrité, confidentialité, protection et résilience, ces vérifications pourront 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.
- 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.

5.5 La mise en place d'une procédure de remontée et de notification des violations de sécurité

Dans la mesure où les organismes Hlm vont être tenus de notifier les violations de données personnelles, la DSI doit s'assurer de la **mise en place d'une procédure de détection des violations de données** à caractère personnel au sein de l'organisme Hlm, et s'assurer également que **les sous-traitants** auxquels les traitements de données à caractère personnel sont confiés, disposent d'une telle procédure.

Contenu du registre des violations de sécurité à tenir :

- faits concernant la violation des données à caractère personnel,
- effets sur le système d'information et sur les personnes concernées,
- mesures prises pour y remédier.

Cette obligation s'applique y compris lorsque les données sont des données pseudonymes ou si elles ont fait l'objet d'un chiffrement pour en assurer la sécurité.

18 ENCADRE

QUATRE ÉTAPES CLÉS AFIN DE RÉPONDRE AUX VIOLATIONS DE DONNÉES À CARACTÈRE

Étape 1 : mise en place d'une organisation appropriée et implication le plus en amont possible des membres du comité de crise afin d'être en mesure de réagir rapidement et efficacement et évaluer l'ensemble des implications de la violation

- Avant même la survenance d'un incident :
  - Prévoir quand, par qui et à quel moment, un incident de sécurité est caractérisé comme une violation de données.
  - Identifier le personnel qui pourra être compétent pour mener des investigations et prendre les premières recommandations.
  - Mettre en place une équipe dédiée (« comité de crise ») incluant le CIL/DPO et des personnes qui auront une expertise suffisante sur le sujet : RSSI, DSI, équipes juridiques, représentant du service opérationnel concerné, service communication, département conformité, conseils externes si besoin...

- Identifier les destinataires d'informations sur la violation que ce soit au sein ou en dehors de la société, régulateurs, assureurs, auditeurs, autorités policières (si la faille implique le vol de données ou toute autre activité répréhensible pénalement).

Étape 2 : notification interne, évaluation et résolution de la violation

- Notification : il convient de prévoir que les violations de données soient systématiquement remontées au CIL/DPO, quelle que soit leur ampleur, ainsi qu'au responsable qui décide de la réunion du comité de crise.
- Analyse/évaluation préliminaire de la violation : détermination de son ampleur, de son caractère récurrent ou non.
- Résolution : parallèlement à l'analyse et à l'évaluation de la violation, il convient d'adopter des mesures appropriées pour trouver la cause de la violation et de réduire les dommages potentiels, tout en préservant les preuves qui pourraient être utiles pour déterminer les causes de la violation et y remédier.

Etape 3 : évaluation du risque associé à la faille

- Les risques causés par la faille doivent être évalués afin de :
  - déterminer comment répondre à la faille ;
  - effectuer la notification à la CNIL (cf. Fiche de synthèse n° 3, page 90)
  - déterminer s'il est nécessaire ou approprié de prévenir les personnes concernées.

- En particulier, l'organisme devra prendre en compte :
  - **les catégories de données personnelles** concernées par la faille. Plus l'information sera « sensible », plus haut sera le risque de dommages auprès des personnes affectées. Une combinaison de données personnelles est généralement plus sensible qu'un simple bloc de données personnelles ;

› l**es conséquences d'une faille sur les obligations légales et contractuelles** (si faille de données couvertes par un secret professionnel ou une obligation de confidentialité (comme les données détenues par les travailleurs sociaux) ;
› **l'impact sur les personnes concernées** du fait de la faille (vol d'identité, perte financière, perte de chance commerciale, ou sociale, humiliation, atteinte à la dignité...) ;
› **les destinataires de l'information**. Le risque est plus élevé si le(s) destinataire(s) est inconnu ou si plusieurs personnes sont concernés (si *les failles permettent la diffusion de données personnelles sur internet*). Si le destinataire est une personne de confiance, ou connue de l'organisme, le risque pourrait être moindre.

EN PRATIQUE

› Avoir mis en place une **procédure incident de sécurité/violation de données**, dans laquelle la DSI pourra qualifier l'incident de sécurité ou non. Ensuite le DPO pourra également ajouter s'il y a eu violation de données ou non.
› **Faire valider** la procédure incident de sécurité auprès de la direction générale après qu'elle ait été complétée.
› Essayer **de trouver les causes** de la faille et les risques de récurrence (problème systémique ou incident isolé).
› **Prendre les mesures techniques et opérationnelles** nécessaires afin de contenir la faille et de limiter les dommages.
› **Déterminer l'étendue de la faille** (le nombre et la nature de destinataires des données ainsi que le nombre de données personnelles perdues, le nombre de personnes concernées, le type de données concernées (« sensibles » ou bien protégées), les conséquences probables pour les personnes concernées, le risque que les données aient été diffusées et continuent de circuler.

Etape 4 : diffusion des bonnes pratiques

Des mesures destinées **à prévenir la survenance de violations de données** doivent être prises, y compris la diffusion de bonnes pratiques auprès des utilisateurs du système d'information.
Par exemple :
› mettre en veille les postes de travail,
› limiter l'usage des disques durs amovibles et clés USB,
› sécuriser tout transfert de données brutes vers l'extérieur via des dispositifs de chiffrement,
› privilégier le dépôt des données sur des plateformes sécurisées, plutôt que l'envoi par courriel.

PARTIE 6

Annexes

GLOSSAIRE
LES NOUVEAUX TERMES *(mise à jour du Cahier Repères n°1)*

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Le règlement 2016/679 du parlement européen et du conseil relatif à la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel et la libre circulation de ces données a été adopté le 27 avril 2016 et entrera en vigueur le 25 mai 2018. Il est d'application directe et remplace la directive 95/46/CE du 24 octobre 1995. **C'est le nouveau texte de référence européen en matière de protection des données à caractère personnel.**

ACTES DÉLÉGUÉS

Selon l'article 290 alinéa 1 du Traité sur le fonctionnement de l'Union européenne :
« *Un acte législatif peut déléguer à la Commission le pouvoir d'adopter des actes non législatifs de portée générale qui complètent ou modifient certains éléments non essentiels de l'acte législatif* ».
La procédure des actes délégués permet au législateur de l'Union européenne de déléguer à la Commission européenne le pouvoir d'adopter des actes non législatifs de portée générale.

CERTIFICATION/ LABEL EN MATIÈRE DE PROTECTION DES DONNÉES

(Article 42 du RGPD)
Processus permettant l'obtention d'un label ou d'une certification délivré 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.

CODE DE CONDUITE EN MATIERE DE PROTECTION DES DONNÉES PERSONNELLES

(Article 40 du RGPD)
Codes élaborés par des associations et autres organismes professionnels destinés à contribuer à la bonne application du règlement et reconnus conformes par les autorités de protection des données. Le respect des codes de conduites contribue à la démonstration de la conformité des traitements. Le « pack de conformité logement social » pourrait devenir à terme un code de conduite ou servir de base à son élaboration.

COMITÉ EUROPÉEN DE PROTECTION DES DONNÉES (CEPD)

(Articles 68 à 76 du RGPD)
Le CEPD remplace le G29. Ce Comité européen de protection des données est composé de l'ensemble des présidents des autorités nationales ainsi que du contrôleur européen à la protection des données (EDPS), qui est vice-président et assure le secrétariat du CEPD.
Contrairement au G29 le CEPD est un organe de l'Union européenne et une entité indépendante disposant de la personnalité juridique dont les avis sont contraignants. Son rôle le plus important sera à la fois d´arbitrer les différends entre les autorités nationales et d'élaborer une doctrine « européenne ».

CONSENTEMENT

(Article 4,11° et 6,1°(a) et 7du RGPD)
Le consentement a un rôle central dans le RGPD. Il constitue en effet 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 de service 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.

DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO) :

(Articles 37, 38 et 39 du RGPD)
Nouveau terme pour désigner les correspondants informatiques et libertés (CIL). Ses missions sont considérablement élargies, le DPO doit notamment veiller à « l'identification du risque lié au traitement, son évaluation en termes d'origine, de nature, de probabilité et de gravité, et l'identification des meilleures pratiques visant à atténuer le risque » (Considérant 77 du RGPD). Sa désignation est obligatoire pour les organismes publics ainsi que pour les autres responsables de traitements, dès lors qu'ils traitent à grande échelle des données particulières ou de données relatives aux infractions

et aux condamnations, aux mesures de sureté, ou qu'ils utilisent de manière systématique et à grande échelle des mesures de profilage à des fins de prise de décision.

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 ANONYMES

(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 législation en matière de protection des données ne s'applique pas aux données « anonymisées ». Elle s'applique en revanche aux données pseudonymes.

DONNÉES PSEUDONYMES

(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 législation en matière de protection des données ne s'applique pas aux données « anonymisées ». Elle s'applique en revanche aux données pseudonymes.

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 ». Cette notion, qui intègre celle de données sensibles (cf. GR n°1) est étendue à de nouvelles catégories de données : les données génétiques, les données biométriques, les données relatives à la vie sexuelle (notion plus large que celle de l'orientation sexuelle).

DONNÉES RELATIVES A 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 *(Article 4 du Règlement 2016/679)*.

DROIT À L'OUBLI

(Article 17 du RGPD)

Droit de la personne concernée d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant.

DROIT À LA PORTABILITÉ

(Article 20 du RGPD)

Obligation pour le responsable de traitement de fournir aux personnes concernées leurs données personnelles collectées auprès de ces derniers « dans un format structuré, couramment utilisé, lisible par machine et interopérable ». 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. *(Article 20 du Règlement 2016/679)*.

ÉTUDE D'IMPACT RELATIVE SUR LA VIE PRIVÉE (EIVP) *(Article 35 du RGPD)*

Méthode d'analyse de conformité et de risque permettant au responsable de traitement de démontrer la conformité des traitements.

LICEITÉ DES TRAITEMENTS

(Article 6 du RGPD)

L'obligation de justifier d'une base légale pour traiter des données à caractère personnel est reconduite dans le RGPD. Pour pouvoir faire l'objet d'un traitement par les organismes Hlm, la collecte des données à caractère personnel doit pouvoir se fonder sur l'une des bases légales suivantes : à savoir le respect d'une obligation légale, l'accomplissement de la mission de service public qui leur est dévolue,

l'exécution de mesures contractuelles, voir même dans certains cas, l'organisme Hlm peut se fonder sur leur intérêt légitime ou celui d'un tiers ou sur la base du consentement de la personne concernée. Les organismes Hlm doivent identifier la base légale du traitement dans le registre des traitements et en informer les personnes concernées.

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.

PRINCIPE DE 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 **limitées à ce qui est nécessaire pour les finalités pour lesquelles elles sont traitées.**

Ce principe est plus strict que le principe de proportionnalité qui laissait une certaine marge d'appréciation. Cela fait notamment référence à la limitation de la conservation des données, au recours à la pseudonymisation et au « privacy by design ».

PROTECTION DES DONNÉES DÈS LA CONCEPTION (PRIVACY BY DESIGN) ET PROTECTION DES DONNÉES PAR DEFAUT (PRIVACY BY DEFAUT)

(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 (*exemple : la purge obligatoire du système, ou l'impossibilité de mémorisation des données bancaires plus de deux 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*).

PRINCIPE DE RESPONSABILITÉ (ACCOUNTABILITY)

(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.

PROFILAGE

(Articles 4,4° et 22 du RGPD)

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 (EIVP, consultations préalables).

Les personnes concernées peuvent par ailleurs s'opposer au profilage à des fins commerciales.

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.

RÈGLES D'ENTREPRISE CONTRAIGNANTE (BCR OU BINDING CORPORATE RULES)

(Articles 46 et 47 du RGPD)

Le RGPD consacre les BCR en tant qu'instrument permettant de transférer des données à caractère personnel au sein d'un groupe de société. Elles peuvent concerner les transferts entre responsables de traitement, mais également ceux réalisés par des prestataires intervenant en qualité de sous-traitant. Leur adoption par des sous-traitants est un gage de respect par ces derniers de la conformité à la législation en matière de protection des données.

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.

TRAITEMENT DE « GRANDE AMPLEUR »

(G29, WP 248, lignes directrices relatives à la conduite d'une EIVP)

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, lignes directrices relatives à la conduite d'une EIVP)

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

› traitement réalisé en application d'un système,
› traitement prédéfinis, organisés ou méthodiques,
› traitements réalisés en tant qu'élément d'une stratégie.

VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

(Articles 4, 12° et 33 du RGPD)

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 (cf. GR n°1). Il y a violation de données à caractère personnel dès lors qu'un évènement quel qu'il soit (de nature technique ou autre) a pour conséquence un défaut de sécurité (i.e. la perte, l'altération, la divulgation ou l'accès non autorisés). Tous les responsables de traitements ont une obligation générale de notifier les violations de données à caractère personnel.

LISTE DES ENCADRES

1 FICHE PRATIQUE
EXEMPLE DE FICHE DE POSTE DU (DE LA) DÉLÉGUÉ(E) À LA PROTECTION DES DONNÉES

Cette fiche vise à décrire les rôles et fonctions de la personne chargée d'assurer le respect de la législation en matière de protection des données personnelles. Elle se base tant sur les dispositions de la Loi Informatique et libertés (art.22) et de son décret d'application (Titre III) ainsi que celles du RGPD du 27 avril 2016 (art. 37 à 39). **La personne occupant les fonctions de délégué(e) à la protection des données personnelles (DPO) est désignée par la direction de l'organisme.**

FONCTIONS

- **Veiller, d'une manière indépendance,** au respect de la législation en matière de protection des données à caractère personnel. À ce titre, il/elle accompagne les opérationnels et l'exécutif dans la prise de décision portant sur la mise en œuvre de traitements de données à caractère personnel et assure le pilotage et déploiement de la démarche de conformité à la législation en matière de protection des données personnelles.
- **Être le point de contact de la CNIL,** ainsi que des personnes concernées par les traitements de données à caractère personnel mis en œuvre : ses coordonnées sont rendues publiques et il reçoit discrètement les plaintes et réclamations des personnes. Il est assujetti pour ses missions à une obligation de confidentialité (sous réserve de la décision du législateur de l'assujettir au secret professionnel).

RESPONSABILITÉS

- **Définir en accord avec la direction :**
  - La gouvernance en matière de protection des données à caractère personnel,
  - L'identification, le recensement et la revue de l'état de conformité des traitements de données à caractère personnel,
  - Les actions à mettre en œuvre aux fins d'assurer la conformité des traitements de données à caractère personnel, et notamment la mise en œuvre des mesures de protection de la vie privée dès la conception et par défaut (« privacy by design et by default ») et la conduite d'études d'impact sur la vie privée.
- **Participer à l'évaluation** des risques associés à la mise en œuvre des traitements, en concertation avec les autres services, en particulier les personnels en charge de la sécurité des systèmes d'information, les services juridiques et conformité, ainsi que les services opérationnels concernés.
- **Informer, conseiller, émettre des recommandations et soutenir** le responsable de traitement afin de lui permettre de respecter la législation en matière de protection des données à caractère personnel.
- **Rédiger,** après consultation des services concernés, **des procédures, lignes directrices et guides pratiques** destinés à assurer le respect de la législation en matière de protection des données à caractère personnel.
- **Concevoir les programmes et actions de formation** des personnels en matière de protection des données à caractère personnel.
- **Assister les services** ayant la responsabilité des traitements de données à caractère personnel à la rédaction des dossiers de formalités et autorisations auprès de la CNIL, ainsi qu'à la tenue à jour du registre des traitements de données à caractère personnel, et de la documentation s'y rapportant.
- **Être le point de contact de la CNIL** pour toute question se rapportant à la protection des données à caractère personnel et le DPO est consulté avant toute intervention/action auprès de la CNIL ou des autres autorités de protection des données
- **Recevoir et instruire**, en concertation avec les services concernés, **les demandes et réclamations** des personnes concernées par les traitements de données à caractère personnel.
- **Assurer une veille législative et règlementaire** en matière de protection des données à caractère personnel et entretenir ses connaissances sur les bonnes pratiques et règles professionnelles applicables.

MOYENS D'ACTION

- **Le DPO est consulté préalablement** à la mise en œuvre ou en cas de modification de traitements de données à caractère personnel, ainsi que sur toute question relative à la protection des données à caractère personnel.

- **Est associé en temps utile** à la conception et au déploiement de nouveaux systèmes et traitements informatiques et participe à la réalisation de études d'impact sur la vie privée, aux groupes de travail internes sur la déclinaison opérationnelle de la réglementation et sur l'optimisation des outils et des processus mis en place.
- **Contrôle le respect des obligations légales et réglementaires**, la mise en œuvre de mesures de « privacy by design », ainsi que la bonne prise en compte de ses conseils et recommandations.
- **Consulte la CNIL en cas de doute** sur l'application de la législation ou des recommandations de la CNIL et des autres autorités de protection des données à caractère personnel,
- **Rend compte directement à la direction** sur l'exercice de sa mission, notamment par la rédaction d'un bilan annuel de son action, et alerte la direction sur les difficultés rencontrées dans l'exercice de ses missions, ainsi que sur les éventuels manquements aux dispositions légales et réglementaires applicables en matière de protection des données à caractère personnel et préconise des mesures permettant de concilier les exigences applicables avec les contraintes métiers.

CONDITIONS D'EXERCICE

- **Indépendance fonctionnelle**

› Le DPO exerce ses mission d'une manière indépendante et à ce titre il/elle ne peut pas être limité dans l'exercice de ses missions telles que définies par la loi, ainsi que dans la présente fiche de poste et les procédures internes par la direction ou les services supports ou opérationnels.

› Il/elle réfère et rend compte de son action directement et exclusivement au plus haut niveau de la direction.

› Il/elle ne peut faire l'objet de sanctions ou de représailles du fait de l'exercice de ses missions.

- **Moyens**

Le DPO dispose de moyens adéquats, notamment humains et budgétaires, et de temps appropriés pour l'exercice de ses missions. En particulier :

› de relais désignés dans les services opérationnels,

› d'un budget propre défini en concertation avec la direction, permettant notamment d'entretenir ses connaissances spécialisées, participer aux réunions organisées par les régulateurs et autorités, mener des actions de sensibilisations, y compris via l'animation d'un page intranet du site.

› d'un pouvoir d'investigation et d'accès aux données à caractère personnel traitées et ses sous-traitants, ainsi qu'aux rapports d'audit relatifs aux opérations de traitements.

› Le DPO peut en outre s'appuyer sur les autres fonctions de conformité et dispose du soutien de la direction.

- **Absence de conflit d'intérêt**

Les missions ou actions exercées concurremment par le DPO ne doivent pas le placer en situation de conflit d'intérêt au regard de ses missions. En particulier, le DPO ne doit pas se trouver en position de responsable de traitement (*i.e. pas d'attributions le conduisant à décider de la mise en œuvre de traitement ou de la définition des finalités et moyens de traitements de données à caractère personnel*).

- **Devoir de confidentialité**

Le DPO est soumis contractuellement à une obligation renforcée de confidentialité en ce qui concerne l'exercice de ses missions, et en particulier dans le cadre de la réception des plaintes et réclamations des personnes concernées.

- **Qualifications et qualités professionnelles**

Le DPO est désigné sur la base de ses qualités professionnelles. **Il/elle :**

› **Justifie d'une connaissance experte et pratique** du droit et des pratiques en matière de protection des données à caractère personnel, ainsi que d'une maîtrise du contexte légal et réglementaire applicable au responsable de traitement.

› **Dispose ou acquiert une connaissance appropriée** en matière de systèmes d'information et de sécurité informatique de nature à lui permettre d'identifier les enjeux et appréhender les recommandation et exigences de la CNIL et autres autorités de protection des données à caractère personnel en la matière.

› **Dispose d'une connaissance approfondie** du statut des organismes Hlm, ainsi que de l'environnement légal et réglementaire applicable au secteur du logement social, et des systèmes d'information utilisés par les organismes Hlm.

2 FICHE PRATIQUE
LES DIFFÉRENCES STATUTAIRES CIL/DPO

STATUT	CIL	DPO	COMMENTAIRE
Obligatoire	Non	Oui	
Plein temps	Non	Non	Le DPO peut exercer d'autres tâches
Indépendance fonctionnelle	Oui	Ouii	Elle doit être garantie par la direction générale
Rattachement au COMEX	Non	Ou	La direction générale doit désigner la personne/la fonction représentant la direction à laquelle le DPO sera rattaché fonctionnellement
Expertise, capacité à accomplir ses missions	Non	Oui	Suppose que les connaissances soient acquises avant la désignation
Externalisation	Condition de seuil	Sans conditions	
Confidentialité/ Secret professionnel	Non	Oui	Le DPO ne doit pas exercer les attributs du responsable de traitement, *ex. décider des moyens du traitement*
À l'abri des conflits d'intérêt	Oui	Oui	
À l'abri des sanctions	Oui	Oui	L'absence de sanctions du fait de l'accomplissement de ses missions doit être garanti par la direction générale
MISSIONS			
Assurer le respect de la législation	Veille	Oui	
Contrôle a priori formalisé pour les traitements « à risques »	Facultatif	Oui	
Sensibilisation	Oui	Oui	
Supervision des audits	Non	Oui	Le DPO pourra recommander la conduite d'audits et leur réalisation pourront lui être confiées par le responsable de traitement
Saisine directe par les personnes concernées	Non	Oui	Le DPO aura un rôle pilote dans la conduite des EIVP
Avis sur les EIVP	Non prévu	Oui	Rôle inchangé
Correspondant de la CNIL	Oui	Oui	La loi Informatique et liberté pourrait maintenir ce droit
Droit d'alerte de la CNIL	Oui	Non prévu	
Coopération avec la CNIL	Non	Oui	
MOYENS			Il s'agit d'une des obligations essentielles du responsable de traitement
Obligation du responsable de traitement de fournir les moyens	Oui	Oui	
Accès aux données à caractère personnel et aux opérations de traitement	Non	Oui	Permet notamment au DPO de traiter les plaintes et réclamations des personnes concernées
Entretiens des connaissances spécialisées	Non	Oui	Obligation de formation continue justifiée par des attestations

3 FICHE PRATIQUE
ÉLÉMENTS DEVANT FIGURER DANS LES MENTIONS D'INFORMATIONS POUR SATISFAIRE À L'OBLIGATION DE TRANSPARENCE

INFORMATIONS DE BASE DEVANT ÊTRE PRÉSENTE SUR TOUTE MENTION (RGPD, ART.13 à 15)

(Les nouveautés introduites par le RGPD apparaissent en gras)

- Identité et coordonnées du responsable de traitement
- Le cas échéant, coordonnées du DPO
- Finalités du traitement
- **Base juridique et identification de l'intérêt légitime poursuivi le cas échéant**
- **Catégories de données personnelles**(2)
- Destinataires ou catégories de destinataires des données à caractère personnel
- Transfert de données + garanties + moyens d'en obtenir une copie des garanties (contrats ou BCR)(1)
- Durée de conservation ou critères permettant de la déterminer(3)

MENTION À APPOSER SEULEMENT SI « NÉCESSAIRE POUR UN TRAITEMENT ÉQUITABLE ET TRANSPARENT »

Droit de demander la rectification, effacement, **limitation** ou droit de s'opposer(1)	*Par exemple :* utilisation des données personnels des locataires fournis via l'accompagnement social à des fins statistiques
Droit à la portabilité(2)	Obligation qui s'appréciera selon le type de document *Par exemple :* service en ligne mettant à disposition des locataires les quittances de loyer
Droit de retirer son consentement(3) **lorsque le traitement est fondé sur le consentement**	*Par exemple :* Possibilité de retirer son consentement dans pour les formulaires de recueil du consentement dans le cadre de l'appréciation des difficultés sociales
Source d'où proviennent les données à caractère personnel et, le cas échéant, une mention indiquant qu'elles sont issues ou non de sources accessibles au public(3)	Concerne les cas de collecte indirecte. *Par exemple :* la vérification de certaines informations communiquées par les locataires à partir de fichiers publics
Droit d'introduire **une réclamation auprès d'une autorité de contrôle**(2)	Il s'agit ici de mentionner le droit de saisir la CNIL d'une réclamation
Caractère réglementaire ou contractuel de la collecte(2)	Il s'agit ici d'indiquer la base légale du traitement. *Par exemple :* la collecte ou la transmission résulte d'une obligation légale de l'organisme Hlm
Caractère obligatoire ou facultatif et conséquences en cas de non réponse	*Par exemple :* questionnaire de satisfaction
Prise de décision automatisée (y compris profilage) + informations utiles sur logique sous-jacente et importance/conséquences sur les personnes concernées(4)	*Par exemple :* mise en œuvre du système de cotation
Intention de procéder à un traitement ultérieur pour une finalité autre(2)	*Par exemple :* enquêtes de satisfaction

(1) Obligation qui s'appréciera selon le type de document : le locataire ne peut pas s'opposer au traitement de ses données aux fins de l'exécution du contrat de bail sauf à rendre impossible cette exécution ; il peut par contre s'opposer au maintien de son nom dans une liste de diffusion et en demander l'effacement
(2) Applicable à la collecte directe uniquement
(3) Rendu obligation par la Loi Informatique et libertés telle que modifiée par la LRN en 2016
(4) Déjà recommandé par la CNIL qui conditionne l'obtention des autorisations délivrées sur le fondement de l'article 25, I, 4° de la Loi Informatique et libertés.

4 FICHE PRATIQUE
EXEMPLE DE GOUVERNACE SOUS FORME DE RACI

		Sponsor DG	Direction	Maîtrise	DPO	RSSI	Relais I et L
R	RESPONSABLE (R) = personne qui assume la responsabilité de la fonction						
A	ASSISTANT ou ACTEUR (A) = personne chargée de la tâche						
C	CONSULTANT (C) = interlocuteurs clés devant être associés						
I	INFORMATION (I) = personne/services devant être informés						
	OBLIGATIONS GENERALES DU RESPONSABLE DE TRAITEMENT AU REGARD DE LA FONCTION Informatique et Libertés						
1.0	Pouvoir de direction sur les traitements	C	R	A	C	C	C
1.1	Adoption des règles générales définissant les acteurs de la fonction I&L et les rôles des divisions supports et métiers	R	A	C	C	C	I
1.2	Adoption de la politique générale de l'organisme en matière de protection des données à caractère personnel	R	A	C	C	C	I
1.3	Définition des politiques de sécurité applicables au traitement de données à caractère personnel	C	A	C	C	C	I
1.4	Définition de la politique de durée de conservation, d'archivage et de suppression des données à caractère personnel	C	A	C	C	C	I
1.5	Déclinaison des politiques au sein de chaque entité, division, service	I	R	C	C	C	C
1.6	Allocation des moyens nécessaires assurer la conformité des traitements	C	R	C	C	C	C
1.7	Détermination des finalités des traitements (<=> expression de besoin)	I	R	C	C		I
1.8	Détermination des caractéristiques des traitements : fonctions, données traitées, destinataires, durée de conservation	I	R	C	C	C	I
1.9	Détermination des moyens des traitements (solution informatique, budget, recours à la sous-traitance, implémentation du privacy by design/by default...)	C	R	C	C	C	I
1.10	Mise en œuvre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des traitements	C	R	C	C	C	I
1.11	Signature des EIVP, des demandes d'avis et autorisation auprès de la CNIL	I	R	C	C		C
1.12	Saisine préalable du DPO avant la mise en œuvre des traitements			R	C		I
1.13	Détermination du circuit de validation préalable à la mise en œuvre de traitements de données à caractère personnel	I	R	I	C	C	C
1.14	Arbitrage des difficultés rencontrées lors de la mise en œuvre des traitements	R	C	C	C	C	C
1.15	Réponse aux plaintes et réclamations des personnes	I	R		C	I	C

R	RESPONSABLE (R) = personne qui assume la responsabilité de la fonction	Sponsor DG	Direction	Maîtrise	DPO	RSSI	Relais I et L
A	ASSISTANT ou ACTEUR (A) = personne chargée de la tâche						
C	CONSULTANT (C) = interlocuteurs clés devant être associés						
I	INFORMATION (I) = personne/services devant être informés						
2.0	Contrôle de conformité des traitements à la loi I&L et aux règles internes à l'organisme	C	R	A	C	C	I
2.1	Détermination de la stratégie en matière de de respect des règles I&L	R	A	C	C	C	I
2.2	Identification et priorisation des points de conformité à la loi I&L	C	R	C	C	C	I
2.3	Recensement des traitements de données à caractère personnel (cartographie)	I	R	A	C	C	C
2.4	Détermination de la sensibilité des traitements (classification) et conduite des EIVP	I	R	A	C	C	I
2.5	Identification des points de contrôle en fonction de la sensibilité des traitements	I	R	A	C	C	I
2.6	Réalisation régulière d'audit des traitements et des sous-traitants/prestataires	I	R	A	C	C	I
2.7	Réalisation des analyses de risque liées aux traitements	I	R	A	C	C	I
2.8	Veiller à la sensibilisation et la formation des personnels	I	R	A	C	C	I
2.9	Vérification du respect des engagements pris auprès de la CNIL au travers des demandes d'avis et autorisations et packs de conformité	I	R	A	C	C	I
2.10	Vérification du respect de l'obligation d'information des personnes	I	R	A	C	C	I
2.11	Vérification de la licéité et la pertinence des données traitées	I	R	A	C	C	I
2.12	Vérification de l'existence de règles de sécurité appropriées à la sensibilité des traitements	I	R	A	C	C	I
2.13	Vérification du respect des durées de conservation et de la politique d'archivage	I	R	A	C	C	I
	OBLIGATIONS SPECIFIQUES EN CAS DE DESIGNATION D'UN DPO						
3.0	Garantie du statut du DPO	R	A	I	C	I	I
3.1	Garantir l'indépendance fonctionnelle du DPO	R	A	I	C	I	I
3.2	Lui allouer des moyens humains, organisationnel et budgétaires suffisants pour assurer ses missions	R	A	I	C	I	I
3.3	Assurer la formation continue du DPO	R	A	I	C	I	I
4.0	Efficacité du dispositif	R	A	A	C	I	I

FICHE DE SYNTHÈSE N°1

LES CHANGEMENTS CONTENUS DANS LE RGPD AFFECTANT LA RÉGULATION

1. Le relèvement du montant des sanctions financières encourues

Le risque de sanction administrative (Cf. Repères n°1, p. 12) est considérablement accru par le RGPD. Les sanctions pécuniaires encourus qui ont été portées à 3 millions d'euros par la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, pourront s'élever, avec le Règlement général relatif à la protection des données, jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial consolidé.

Le RGPD prévoit par ailleurs que les sanctions financières doivent être effectives, proportionnées et dissuasives et tenir compte de chaque cas particulier. **Les montants varient selon les manquements à la législation relative à la protection des données à caractère personnel :**

€ 10 millions ou jusqu'à 2% CA mondial consolidé	€ 20 millions ou jusqu'à 4% CA mondial consolidé
› Consentement des mineurs › Traitements ne nécessitant pas l'identification › Protection des données dès la conception et protection par défaut › Désignation des responsables conjoints du traitement › Désignation des sous-traitants › Désignation des représentants des responsables du traitement ou des sous-traitants non UE › Désignation sous l'autorité du Responsable de traitement ou du sous-traitant › Non-tenue du registre › Coopération avec la CNIL à sa demande › Garantie de la sécurité du traitement › Notification à l'autorité de contrôle d'une violation de données à caractère personnel › Communication à la personne concernée d'une violation de données à caractère personnel › Tenue d'une EIVP › Tenue d'une consultation préalable › Désignation du DPO › Fonctions du DPO › Missions du DPO › Non-respect d'une certification › Non-respect des exigences soumises aux organismes de certification › Manque de contrôle des codes de conduites par l'organisme désigné	› Conditions de licéité › Principes de base › Règles de consentement › Traitement des données particulières › Non-respect des droits des personnes › Transfert de données sans garanties adéquates › Traitement du NIR › Droit d'accès aux documents administratifs › Données relatives aux employés › Archives publiques, recherche et statistiques › Non-respect du secret professionnel › Règles applicables aux églises et associations religieuses › Non-respect d'une injonction de la CNIL

2- Les facteurs qui devront être pris en compte par les autorités de contrôle pour décider du montant de la sanction

Mesures atténuantes	Mesures aggravantes
› violation commise par négligence › mesure prise pour atténuer le dommage subi par les personnes concernées › degré de responsabilité › mise en œuvre du privacy by design/by default › mesures prises pour assurer le respect de l'obligation de sécurité › degré de coopération avec la CNIL en vue de remédier à la situation et en atténuer les conséquences négatives › l'application de codes de conduite ou de mécanismes de certification approuvés › respect de ces mesures ordonnées par l'autorité de protection en application de ses pouvoirs de sanction	› nature, la gravité et la durée de la violation › le fait que des données particulières ou données relatives aux infractions, condamnations et mesures de sûreté soient concernées, › nombre de personnes concernées affectées › niveau de dommage qu'elles ont subi › violation délibérée › existence de violation précédentes › avantages financiers obtenus ou les pertes évitées du fait de la violation › absence de notification de la violation

3-Le remplacement du groupe de l'article 29 (G29) par le Comité européen pour la protection des données (CEPD)

Le Comité européen de protection des données est composé de l'ensemble des présidents des autorités nationales ainsi que du contrôleur européen à la protection des données (EDPS), qui est vice-président de droit du Comité européen. Contrairement au rôle du G29, le CEPD n'est pas un simple comité de conseil mais une entité indépendante avec sa propre personnalité juridique qui pourra rendre des avis contraignants. Son rôle le plus important sera à la fois d´arbitrer les différends entre les autorités nationales et d´élaborer une doctrine « européenne ». Par ailleurs, il promeut la coopération entre les différentes autorités de contrôles, publie des lignes directrices, recommandations et des « bonnes pratiques ». L'ensemble de ces nouvelles fonctions permettent au CEPD de jouer un rôle clé dans la l'application uniforme du RGPD au sein de l'Union européenne.

4- La reconnaissance du droit à une réparation effective pour les personnes concernées

Le RGPD (art.62) reconnait aux personnes concernées le droit d'obtenir du responsable de traitement ou du sous-traitant réparation du préjudice matériel ou moral subi. Ainsi, lorsque plusieurs responsables du traitement ou lorsque, un responsable du traitement et un sous-traitant participent au même traitement et qu'ils sont responsables d'un dommage causé par le même traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité vis-à-vis de la personne concernée.

5- L'introduction d'une action collective en matière de violation de la loi Informatique et Libertés

Anticipant sur l'entrée en application du Règlement général relatif à la protection des données qui prévoit en son article 80, 2°le principe d'actions de groupela loi n° 2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIe siècle consacre (*nouvel art. 43ter de la Loi Informatique et libertés*) l'extension de l'action collective aux personnes concernées par les traitements de données à caractère personnel. Elle permet aux personnes concernées via les associations agréées d'obtenir le prononcé d'une injonction de cesser, ou de faire cesser le manquement, et de prendre dans un délai que le juge fixe toutes les mesures utiles à cette fin, une astreinte pouvant être ordonnée par le juge.

FICHE DE SYNTHÈSE N°2

LA PRISE DE DÉCISION AUTOMATISÉE (PROFILAGE) : IMPACTS SUR LA COTATION DES DEMANDEURS

Les restrictions portant sur la **prise de décision automatisée** ne sont pas nouvelles. Elles figuraient déjà dans la Loi Informatique et libertés (art.10).

Le texte adopté dans le RGPD (71ème et 72ème Cons et art.4, (4) et art.22) vise **spécifiquement** les cas où le profilage est utilisé dans le cadre **d'une prise de décision** basée uniquement sur **un traitement automatisé** et produisant des effets juridiques opposables à la personne concernée.

La notion de profilage est introduite par le RGPD : elle vise les traitements destinés à évaluer la personnalité, ainsi que les traitements prédictifs. Les restrictions s'appliquent dès lors qu'une décision est prise ou que des conséquences juridiques **affectent de manière significative l'intéressé**.

Les traitements concernés à titre principal par les dispositions relatives au profilage sont ceux visés actuellement par le régime de l'autorisation de l'article 25 de la Loi Informatique et libertés, à savoir ceux permettant la détection et la prévention de la fraude, des impayés ou des incidents.

- sont compris : les scores de risques, la gestion des incivilités, les fichiers de mauvais payeur ou de « personnes à risque » d'une manière générale (« les listes noires »),
- les systèmes de cotation dans le cadre de la gestion de la demande et des attributions.

Illustration

Les mesures techniques et organisationnelles devant être mises en œuvre doivent comprendre :

- audits réguliers de gestion des habilitations ;
- la pseudonymisation et le chiffrement des données à caractère personnel ;
- audit régulier de la journalisation des connexions ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité des systèmes de traitement de données à caractère personnel. Cela comprend la résilience constante des systèmes (*i.e. la capacité de rétablissement à l'identité sans délai après un incident*).
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.
- la détection de toute violation ou intrusion.

Conséquences

- Disposer d'une filière « sécurité des systèmes d'information » (SSI) chargée d'établir et faire appliquer les politiques de sécurité définies au niveau du groupe (peut-être externalisée)
- Assurer l'implication de la filière SSI dans la mise en œuvre des projets informatiques
- Aller progressivement vers la formalisation d'une politique SSI
- Disposer d'une procédure de rédaction d'une « fiche de sécurité », d'un projet informatique destiné à identifier et évaluer les points particuliers de sécurité d'un projet
- Veiller à disposer pour chaque traitement actuellement mis en œuvre d'une documentation à jour relative aux conditions spécifiques de sécurité du traitement afin d'être en mesure de démontrer la conformité avec les standards de sécurité applicables
- 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
- Assurer la sensibilisation des équipes informatiques sur l'intégration de mesures de protection de la protection de vie privée dès la conception dans la démarche de sécurité (« security by design »)
- Disposer d'une politique d'audit des systèmes d'information
- Tenir un journal des incidents.

RGPD, 39ème cons., art. 25, 2°, art.32 et 33
RGPS
CNIL / ANSSI : guides sécurité

FICHE DE SYNTHÈSE N°3

LA NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

Le Règlement général relatif à la protection des données introduit pour les responsables de traitements une obligation générale de notifier **les violations de données à caractère personnel.** De même, le sous-traitant doit alerter et informer sans délai le responsable du traitement en cas de violation de données à caractère personnel. Le responsable du traitement doit **documenter** toute violation de données à caractère personnel, et la tenir à la disposition de la CNIL.

Obligation de notification à la CNIL

Délai : La notification auprès de la CNIL doit être effectuée dans les meilleurs délais et si possible 72 heures au plus tard après en avoir pris connaissance, de la constatation de la violation. Passé ce délai, le responsable de traitement doit justifier des motifs du retard.

- Le défaut de notification peut entraîner des sanctions pouvant aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires mondial consolidé.

Contenu

- La nature de la violation, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés.
- Les mesures à prendre pour atténuer les éventuelles conséquences négatives de la violation de données.
- Les conséquences probables de la violation des données.
- Les mesures à prendre ou prises pour remédier à la violation, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.
- Communiquer les coordonnées du DPO ou d'un point de contact.

Obligation de notification à la personne concernée

Délai : sans délai (peut-être modulé s'il est prioritaire de limiter les risques de propagation).

Modalités : notification individuelle

- à la place il peut être exigée une campagne publique d'information dans les journaux, à la télévision.

Exception : l'obligation de notifier aux personnes concernées ne s'applique pas :

- si la violation en question n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques,
- lorsque le responsable de traitement avait pris des mesures appropriées organisationnelles et techniques (exemple : chiffrement des données),
- lorsque cela entraînerait des efforts disproportionnés.

RGPD, 85ème et 88ème Cons., art. 34

FICHE DE SYNTHÈSE N°4

LA RÉUTILISATION DES DONNÉES À DE NOUVELLES FINS QUE CELLES POUR LESQUELLES LES DONNÉES ONT ÉTÉ INITIALEMENT COLLECTÉES

Le traitement de données à caractère personnel pour d'autres finalités que celles pour lesquelles les données à caractère personnel ont été collectées initialement n'est autorisé que s'il est compatible avec les finalités pour lesquelles les données à caractère personnel ont été collectées initialement. Si ce principe figurait déjà dans la Loi Informatique et libertés, le règlement intègre **le test de compatibilité** déjà préconisé par les autorités de protection des données.

Si le traitement est **nécessaire à l'exécution d'une mission d'intérêt public** ou relevant de **l'exercice de l'autorité publique** dont est investi le responsable du traitement, le droit de l'Union européenne ou le droit d'un État membre peut déterminer et préciser les missions et les finalités pour lesquelles le traitement ultérieur devrait être considéré comme compatible et licite.

Le règlement introduit par ailleurs une présomption de compatibilité pour le traitement ultérieur à des fins **archivistiques dans l'intérêt public,** à des fins de **recherche scientifique ou historique** ou à des fins **statistiques**. Il faut toutefois que cette utilisation soit entourée de garanties appropriées pour les droits et libertés des personnes (telles des mesures de protection de la vie privée dès la conception intégrant le principe de minimisation, dont la pseudonymisation.)

- **Exemple :** lors de l'utilisation du fichier locataire pour l'accession sociale, il est préconisé d'informer la personne concernée qu'elle a un droit d'accès, de modification, de suppression ; que la durée de conservation de ses données est de 3 ans maximum et conformément à la déclaration NS48 en vigueur.

À NOTER

Le test de compatibilité

- existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;
- contexte dans lequel les données à caractère personnel ont été collectées (en particulier, relation entre la personne concernée et le responsable de traitement) ;
- nature des données à caractère personnel (données sensibles ou données relatives à des condamnations pénales et à des infractions) ;
- conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
- existence de garanties appropriées (chiffrement, pseudonymisation...).

Loi Informatique et Libertés, art.6
RGPD, 50ème Cons., art.5, 1°, b), art.89

FICHE DE SYNTHÈSE N°2

LE NOUVEAU DROIT À LA PORTABILITÉ : UN ÉLÉMENT À PRENDRE EN COMPTE DANS LE DÉPLOIEMENT DE L'INTERNET DES OBJETS

Parfois présenté comme un dérivé du droit d'accès, le droit à la portabilité est en réalité un droit autonome dont les critères d'application sont spécifiques et dont la portée va au-delà de celle généralement reconnue aux droits des personnes par la législation en matière de protection des données personnelles. **Ce droit vise à renforcer le contrôle qui est exercé par les personnes concernées sur leurs données.** Il comporte pour se faire deux volets.

- En premier lieu ce droit oblige le responsable de traitement à fournir aux personnes concernées leur données personnelles de manière « ***lisibles, structurés et facilement lisible par une machine interopérable*** » afin de faciliter la portabilité des données.
- En second lieu, ce droit donne également **la possibilité pour la personne concernée de demander que les données soient transmises directement par le premier responsable de traitement au second,** lorsque cela est techniquement possible. Le responsable de traitement a par ailleurs l'obligation d'information sur l'existence du droit à la portabilité au moment de la collecte ainsi que lorsque la personne concernée demande l'effacement de ses données ou survient la fin du contrat.

Exemple : la mise à disposition des locataires d'applications associées à des objets connectés à des fins de contrôle des dépenses énergétiques pourrait faire naître un droit à la portabilité en faveur des locataires **à la condition que le bailleur détienne les données et les conserve**.

Conditions d'ouverture du droit à la portabilité	Les conséquences pour les organismes Hlm
Le traitement doit être automatisé Le traitement doit avoir pour fondement légal le consentement de la personne ou la nécessité contractuelle Le traitement doit porter sur des données à caractère personnel Les données doivent avoir été « fournies » par la personne concernée Le droit à la portabilité ne vise pas que les données volontairement transmises par la personne concernée, mais également des données générées et collectées à partir de l'interaction avec la personne concernée *(par exemple, logs de connexion, métadonnées, historique d'une transaction).* Le G29 considère que sont en revanche exclues, les données qui sont dérivées ou déduites, comme les données de profilage, ou même les données de trafic *(géolocalisation, données de traçage via des cookies par exemple).*	Nécessité d'identifier en amont les traitements pour lesquels le droit à la portabilité s'applique Vérifier que les mentions d'informations visent le droit à la portabilité Mettre en place une procédure visant à informer le locataire sur ce droit en cas de départ du logement Vérifier que les données à caractère personnel concernées (y compris les métadonnées) peuvent être exportée dans un format permettant l'interopérabilité Si possible, rendre l'exercice du droit à la portabilité directement accessible à partir d'un extranet RGPD : 68ème Cons. art. 20, 20, 2° et 20, 3°, 13, 2° (b) et 14 2° (c) G29 : lignes directrices 2017, WP 242 2017, wp 242 (disponibles en anglais)

La collection des Cahiers, toute l'expertise de l'Union sociale pour l'habitat

PERSPECTIVES
RÉFÉRENCES
REPÈRES
SIGNETS
ACTES

Une déclinaison par thématique

- accession sociale
- aménagement et urbanisme
- communication
- droit et fiscalité
- énergie et environnement
- habitants/locataires
- maîtrise d'ouvrage
- patrimoine
- politiques sociales
- qualité de service
- ville et renouvellement urbain

DERNIÈRES PARUTIONS

COLLECTION RÉFÉRENCES

3• L'investissement des organismes Hlm dans la rénovation énergétique. Analyse d'un panel de dossiers de prêts de la Caisse des Dépôts entre 2009 et 2014, *juin 2016*

4• Enseignements du Programme d'instrumentation de l'OPE, *septembre 2016*

COLLECTION REPÈRES

10• Transformation du bâti et amélioration énergétique : comment impliquer les habitants ? *septembre 2015*

11• Habitat à performance énergétique renforcée : évolution des métiers et besoins en compétences, *novembre 2015*

12• Les secteurs de mixité sociale inscrits dans les PLU : un levier au service de la production du logement social, *janvier 2016*

13• Coopération public-public : guide des organismes d'Hlm et de leurs partenaires d'intérêt général, *mars 2016*

14• Guide pour la prise en compte de la biodiversité dans les métiers du logement social, *mars 2016*

15• Systèmes de gestion des données relatives à l'amiante, *mars 2016*

16• Quelle organisation mettre en place pour maîtriser le risque amiante ? *avril 2016*

17• Orientations d'attribution et convention d'équilibre territorial : contribution des organismes Hlm au diagnostic de l'occupation et du fonctionnement du parc social et à l'analyse des enjeux de mixité, *avril 2016*

18• Journal des locataires : tendances et bonnes pratiques, *mai 2016*

19• Plan d'actions Développement durable 2010-2015. Focus sur les actions phares du Mouvement Hlm, *juin 2016*

20• Mobilité résidentielle : l'action des organismes Hlm, *juillet 2016*

21• Les usages des outils de production du foncier pour le logement social : Nice Côte d'Azur Métropole, Lyon Métropole, CA de Plaine Commune, *août 2016*

22• Accompagner le vieillissement des locataires : l'action des organismes d'Hlm Les enseignements du concours « Hlm partenaires des âgés », *septembre 2016*

23• Hébergement, accès au logement et accompagnement social : les partenariats entre bailleurs sociaux et associations d'insertion, *septembre 2016*

24• Habitat social et santé mentale : cadre juridique et institutionnel, pratiques et ressources, *octobre 2016*

25• La communication peut-elle faire évoluer les pratiques ? *décembre 2016*

26• Les éléments constitutifs de l'attractivité des produits en accession sociale, *janvier 2017*

27• Le management des organismes Hlm : réalités, pratiques et enjeux, *janvier 2017*

28• La conduite des projets de gestion de site dans les organismes, *février 2017*

29• Analyse du volet logement de la loi Egalité et Citoyenneté, *février 2017*

30• Incidences des plans de prévention des risques sur les stratégies patrimoniales des organismes Hlm, *mars 2017*

31• Prise en compte de la question de l'amiante dans les contrats d'assurance et la gestion des sinistres, *mars 2017*

32• Densification des emprises foncières existantes : un nouveau gisement pour la production ? *mars 2017*

33• La vidéoprotection et la vidéosurveillance dans l'habitat social, *avril 2017*

34• Enjeux de la maquette numérique dans le logement social, *mai 2017*

35• Les marchés des organismes Hlm : passation et exécution, *mai 2017*

36• Le numérique : levier d'amélioration du service au sein du parc social, *juillet 2017*

37• La tranquillité résidentielle et le partenariat de sécurité publique, *septembre 2017*

38• Réforme du droit des contrats : analyse et conséquences, *septembre 2017*

39• Améliorer et optimiser le montage d'opérations en neuf et en réhabilitation, *septembre 2017*

40• Les achats pour favoriser l'insertion et l'emploi, *septembre 2017*

COLLECTION SIGNETS

4• L'accession sociale sécurisée dans les quartiers en renouvellement urbain, *avril 2016*

5• Logement intermédiaire : décryptage du cadre juridique et fiscal, *mai 2016*

6• Formaliser une engagement qualité de service, *septembre 2016*

7• La médiation des litiges de la consommation dans le secteur Hlm, *novembre 2016*

8• Favoriser les éco-comportements des habitants du logement social, *septembre 2017*

COLLECTION PERSPECTIVES

1• Construire pour gérer : une spécificité de la maîtrise d'ouvrage Hlm - Regards croisés d'acteurs, *septembre 2015*

2• RSE et DSU au service de la stratégie d'entreprise, *octobre 2016*

COLLECTION LES ACTES

9• Solidarités territoriales et habitat : quelles réalités, quel avenir ? *Journée d'étude du 1er juillet 2015*

10• Quoi de neuf chercheurs ? *3èmes rencontres nationales, Paris, 17 novembre 2015*

11• Quoi de neuf acteurs ? *Journée d'actualité du réseau des acteurs de l'habitat, Paris, 10 mars 2016*

12• Loger les jeunes dans le parc social, *Journée professionnelle, Paris, 31 mai 2016*

13• Quoi de neuf chercheurs ? *4èmes rencontres nationales, Paris, 17 novembre 2016*

14• Les Hlm face aux crises : comment gérer, comment communiquer ? *Journée professionnelle du 23 mai 2017*

15• Maquette numérique et changements organisationnels : de l'industrie au bâtiment *Colloque national, Paris, 3 mai 2017*

Vous pouvez commander des exemplaires de ce Cahier en envoyant un bon de commande à H'Prom (**florence.walach@h-prom.fr**).
L'ensemble des Cahiers est disponible en PDF sur http://ressourceshlm.union-habitat.org, après identification de l'utilisateur.

L'UNION SOCIALE POUR L'HABITAT
14, rue Lord Byron • 75384 Paris Cedex 08
Tél. : 01 40 75 78 00 • Fax : 01 40 75 79 83
www.union-habitat.org

L'UNION SOCIALE POUR L'HABITAT
Les Hlm, habiter mieux, bien vivre ensemble