GUIDE PRATIQUE D'ACCOMPAGNEMENT POUR LA PROTECTION DES DONNÉES PERSONNELLES A L'USAGE DES COOPÉRATIVES HLM

JUIN 2018

les COOP' HLM

Avant-propos

La Fédération des sociétés coopératives HLM a conçu ce guide pratique pour vous accompagner dans la mise en œuvre du nouveau Règlement européen sur la protection des données personnelles entré en vigueur le 25 mai 2018.

Ce document est à l'usage des petites entreprises, il a pour objectif de donner les principales clefs pour réaliser votre propre dispositif de protection des données. Il a été conçu à partir des documents émis par la Commission Nationale de l'Informatique et des Libertés (CNIL)[1] et par l'Union Sociale pour l'Habitat[2] Il en reprend les définitions et les cadres d'actions, pour faciliter la lecture, les reprises ne feront pas l'objet de citations systématiques.

Il est composé de 5 parties :

- Les principes du RGPD,
- Les définitions essentielles,
- Les 4 actions principales à mener,
- Le Délégué à la protection des données,
- Des exemples concrets de fiches pratiques de traitement à intégrer dans le registre de traitement ou de mentions.

Des annexes complètent ce guide.

[1] Guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises - Avril 2018 - CNIL
[2] Cahier repères numéro 41 – Octobre 2017 -Union sociale pour l'Habitat

Sommaire

I- Les principes du Règlement sur la protection des sonnées (RGPD)

Le règlement sur la protection des données personnelles est entré en vigueur le 25 mai 2018. Il renforce les droits des personnes et responsabilise davantage les organismes publics et privés, dont les entreprises, qui traitent des données personnelles.

Comme l'indique la CNIL, « si les données personnelles ne sont pas au cœur de votre activité, les moyens à déployer pour vous mettre en conformité au RGPD ne seront pas très importants ».

Pour les coopératives HLM, il va s'agir essentiellement d'analyser les données collectées et leur traitement afin d'assurer sécurisation et protection de ces données.

A) Qui est concerné

Le RGPD s'applique à toute **organisation, publique et privée**, qui traite des données personnelles pour son compte ou pour des tiers, dès lors :

- qu'elle est établie sur le territoire de l'Union européenne ;
- que son activité cible directement des résidents européens.

Le RGPD concerne aussi les **sous-traitants** qui traitent des données personnelles pour le compte d'autres organismes.

En pratique : si vous traitez ou collectez des données pour le compte d'une autre coopérative ou d'un organisme Hlm, vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées. De plus, si vous confiez la gestion des prospects ou de vos salariés à une autre entreprise, vous êtes aussi concernés car vous êtes considérés comme le responsable du traitement.

B) La responsabilité

Le RGPD met fin au régime de droit commun de déclaration prévu par la loi Informatique et Libertés et repose sur le principe de **responsabilité** des organisations. Il s'agit pour la coopérative de prouver la mise en place de mesures permettant d'assurer la confidentialité et la sécurité des données traitées. En cas de contrôle, la coopérative doit être en mesure de démontrer à la CNIL qu'elle se conforme à ses obligations. En absence de cette mise en conformité, les sanctions peuvent aller jusqu'à 4% du Chiffre d'affaire annuel.

En pratique : La coopérative doit désormais justifier de l'existence et de la fiabilité de leurs procédures relatives à la collecte, l'usage, la protection, le stockage, l'anonymisation ou encore la suppression des données à caractère personnel. Elle doit pouvoir à tout moment démontrer le respect des obligations du règlement.

Pour cela, elle devra tenir un registre des traitements des données à caractère personnel, réaliser un bilan annuel si elle a choisi d'avoir en son sein un délégué à la protection des données (DPD) et enfin documenter toutes les actions supplémentaires entreprises par la coopérative : formation, charte informatique, dispositif de sécurisation informatique…

Le RGPD introduit la notion de **responsabilité conjointe**. Elle vise à responsabiliser les différents acteurs du traitement des données à caractère personnel. Il est ainsi 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.

C) La transparence

Le RGPD renforce les droits (droit à l'oubli, à l'effacement, à la portabilité[3],…) des citoyens européens en leur donnant plus de contrôle sur leurs données personnelles. Cela se traduit en particulier par la mise en œuvre du principe de **transparence** sur les données collectées et leur traitement.

En pratique : Le responsable de traitement devra veiller à inclure une mention visible, accessible, compréhensible et concise sur les documents de recueil de données personnelles : prospect, clients, coopérateurs, salariés …

En pratique : 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[4].

D) La confiance

L'approche du RGPD est fondée sur la notion de gestion des risques, ce qui permet à la coopérative de définir elle-même les solutions qui correspondent à ses activités. Cette approche repose sur le principe de **confiance** envers les entreprises. La coopérative doit pouvoir montrer les mesures qu'elle a prise pour la protection des données des données personnelles dès la **conception de tout traitement** comportant ces données et tout au long de son développement («privacy by design and by default»). Il en résulte un contrôle plus exigeant des conditions de licéité[5] autorisant le traitement des données à caractère personnel. Les traitements mis en œuvre doivent être licites et pour cela répondre à certaines conditions comme par exemple :

- la personne concernée a **consenti** au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;
- le traitement est nécessaire à **l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
- 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.

En pratique : Lors de la conception du traitement et tout au long de son développement, le responsable de traitement veillera à ne collecter et traiter des données qu'en fonction de finalités déterminées, explicites et légitimes. De plus, il ne sera collecté que les données pertinentes et nécessaires au regard des finalités poursuivies. Enfin, les données devront être exactes et mises à jour si nécessaire suivant un processus clairement défini.

[3] Le droit à la portabilité offre aux personnes la possibilité de récupérer une partie de leurs données dans un format ouvert et lisible par machine. Elles peuvent ainsi les stocker ou les transmettre facilement d'un système d'information à un autre, en vue de leur réutilisation à des fins personnelles.
[4] Cahier repère numéro 41- Union sociale pour l'habitat.
[5] Description de la licéité d'un traitement en annexe.

E) La conservation des données

Le RGPD repose aussi sur le principe de la limitation de la conservation des données. En effet, la conservation des données permettant l'identification des personnes concernées ne doit pas excéder la durée nécessaire aux finalités pour lesquelles elles sont enregistrées.

En pratique : La coopérative devra mettre en œuvre une procédure pour effacer les données dont elle n'aura plus l'usage dans l'exercice de ses activités. Dans les exemples proposés en partie 5, il est proposé des durées de conservation des données.

II- Les définitions essentielles

A) Donnée personnelle

Pour la CNIL, une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ». Une personne peut être identifiée :

- **directement** (exemple : nom, prénom) ;
- **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- **à partir d'une seule donnée** (exemple : numéro de sécurité sociale, ADN) ;
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association).

Par ailleurs, sont considérées comme **sensibles** les données révélant les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle d'une personne. Leur traitement est en principe interdit sauf dans certains cas tels que :

- Si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée),
- Si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL.

En pratique: des données sensibles peuvent être collectées pour la mise en œuvre d'un accompagnement social personnalisé.

B) Traitement de données personnelles

L'article 4 du RGPD définit un **traitement** comme " toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction".

En pratique: La tenue d'un fichier informatisé ou « papier » qui collecte les coordonnées de prospects via un questionnaire est un exemple de traitement, mais cela peut aussi être une liste de messagerie.

III- Les 4 actions principales à mener

Les actions retenues issues sont issues du guide pratique de sensibilisation au RGPD pour les petites et moyennes entreprises, réalisé par la CNIL et déjà cité.

A) Recensez les fichiers

Le registre des activités de traitement permet de recenser vos traitements de données et de disposer d'une vue d'ensemble de ce que vous faites avec les données personnelles. Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité.

La réglementation n'exige pas la tenue d'un tel registre pour les organismes de moins de 250 salariés. Mais en pratique, cette dérogation est limitée à des cas très particuliers de traitement et l'obligation est maintenu pour les traitements de gestion de la paie, gestion des clients ou des prospects, données sensibles…

Les coopératives HLM doivent donc mettre en place un tel registre.

Pour cela,

- Identifiez les activités principales de votre entreprise qui nécessitent la collecte et le traitement de données (exemples : gestion du personnel, gestion de la paye, gestion des clients prospects, etc.).
- Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :
    - le nom du responsable de traitement, les coordonnées du Délégué à la protection des données (DPD) ;
    - l'objectif poursuivi (la finalité - exemple : la fidélisation client) et le fondement légal de la collecte;
    - les catégories de données utilisées (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;
    - qui a accès aux données (le destinataire - exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
    - la durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).

Le DPD est décrit dans le chapitre 4.

En pratique : Dans le registre simplifié proposé par la CNIL, le nom du responsable de traitement, les coordonnées du DPD sont à indiquer en début de registre et valables pour toutes les fiches.

Le registre est placé sous la responsabilité du dirigeant de l'entreprise.

Vous n'avez pas en revanche à mentionner au registre les traitements purement occasionnels (exemple : fichier constitué pour une opération événementielle ponctuelle comme la première pierre d'une opération).

Le registre doit être tenu par les responsables de traitement ou les sous-traitants eux-mêmes. Ils peuvent ainsi disposer d'une vue d'ensemble de toutes les activités de traitement de données à caractère personnel qu'ils effectuent.

Une personne au sein de la coopérative peut être spécifiquement chargée de la tenue du registre. Dans le cas où la coopérative a désigné un délégué à la protection des données (DPD), interne ou externe, celui-ci est chargé de la tenue du registre. Le registre pourra ainsi constituer l'un des outils permettant au délégué à la protection des données (DPD) d'exercer ses missions de contrôle du respect du RGPD ainsi que d'information et de conseil du responsable du traitement ou du sous-traitant.

Le registre doit être mise à jour régulièrement au gré des évolutions fonctionnelles et techniques des traitements de données. En pratique, toute modification apportée aux conditions de mise en œuvre de chaque traitement inscrit au registre (nouvelle donnée collectée, allongement de la durée de conservation, nouveau destinataire du traitement, etc.) doit être portée au registre.

En pratique : Un exemple de registre de traitements est proposé en partie 4. Le format du registre est libre. Il est peut-être réalisé au format papier ou électronique. La CNIL propose un format sous Excel ou sous Word.

Un registre spécifique pour les activités de sous-traitance des données personnelles

Si votre coopérative agit à la fois en tant que sous-traitant et responsable de traitement, votre registre doit donc clairement distinguer les deux catégories d'activités.

En pratique, dans cette hypothèse, la CNIL vous recommande de tenir 2 registres :

- un pour les traitements de données personnelles dont vous êtes vous-même responsable,
- un autre pour les traitements que vous opérez, en tant que sous-traitant, pour le compte de vos clients.

En cas de responsabilité conjointe entre une entreprise et son sous-traitants, il est nécessaire de définir dans une convention les obligations réciproques afin d'assurer la conformité au règlement (rôle de chacun et relations vis-à-vis des personnes concernées) et d'assurer la transparence sur cette répartition auprès des personnes concernées, notamment en ce qui concerne l'exercice des droits des personnes concernées (information, accès et rectification).

B) Faites le tri dans les données recueillies

Pour chaque fiche de registre créée, vous devez vérifier :

- que vous êtes autorisés à traiter ces données (vérification du fondement légal (Annexe C)) ;
- que les données que vous traitez sont nécessaires à vos activités, ce sont les principes de responsabilité et de confiance qui s'appliquent ici traduits par « privacy par design » et « privacy par default »
- que vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter ;
- que seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- que vous ne conservez pas vos données au-delà de ce qui est nécessaire.

En pratique : Vous devez vous interroger sur la pertinence des données collectées et leur durée de conservation. Est-ce utile et pertinent de garder des données de prospects non mises à jour plusieurs années ? C'est l'occasion de mettre en œuvre des procédures d'effacement ou d'archivage si nécessaire.

C) Respectez les droits des personnes

Le respect des droits des personnes passe par deux actions principales : l'information des personnes et la possibilité d'exercice de leurs droits.

L'information des personnes peut être en œuvre ainsi : à chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.

Vérifiez que l'information comporte notamment les éléments suivants :

- pourquoi vous collectez les données;
- ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous, de votre « intérêt légitime ») ;
- qui a accès aux données (indiquez des catégories : les services internes compétents, un prestataire, etc.) ;
- combien de temps vous les conservez (exemple : « 5 ans après la fin de la relation contractuelle ») ;
- les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié).

En pratique : Le site internet de la CNIL vous permet de générer automatiquement les mentions que vous souhaitez portées sur vos formulaires.

Exemple de mail reçu par les abonnées du Journal Le Monde :

Chers lecteurs,

La réglementation applicable aux données personnelles évolue, avec l'entrée en vigueur, le 25 mai 2018, du Règlement général sur la protection des données (RGPD), adopté par le Parlement européen.

C'est l'occasion pour *Le Monde* de réaffirmer ses engagements en matière de confidentialité de vos données personnelles et de respect de vos choix s'agissant de leur utilisation.

En prévision de l'entrée en vigueur du RGPD, nous avons mis à jour notre politique de protection des données personnelles. Nous vous invitons à en prendre connaissance.

Nous tenions à vous informer précisément et en toute transparence de ces changements. Nous avons également désigné au sein de notre groupe de presse un délégué à la protection des données, interlocuteur privilégié pour répondre à toutes vos questions en la matière.

Pour le contacter : dpo@groupelemonde.fr

Nous vous remercions de votre confiance.

L'exercice des droits des personnes sur leurs données (droits d'accès, de rectification, d'effacement …) doit être effectif. Pour cela, vous devez mettre en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

En pratique : si vous disposez d'un site web, prévoyez un formulaire de contact spécifique, un numéro de téléphone ou une adresse de messagerie dédiée.

Exemple de mail à envoyer à des abonnés à une newsletter :

Bonjour,

Nous mettons à jour notre politique de confidentialité, en application du nouveau Règlement Général sur la Protection des Données (RGPD) entrant en vigueur dans l'Union Européenne le 25 mai 2018.

Dans ce cadre, nous vous permettons de ne recevoir de notre part que les informations que vous souhaitez recevoir.

Si vous voulez continuer à recevoir la newsletter de *LACOOP.COM*, ne changez rien.

Si vous souhaitez vous désabonner et ne plus recevoir ces actualités, cliquez sur le bouton suivant :

Se désinscrire

N.B : sans désabonnement de votre part avant le 25 mai 2018, vous serez automatiquement reconduit dans notre base de données.

D) Sécurisez les données

La coopérative est tenue d'assurer la sécurité des données personnelles détenues. Bien entendu, les mesures à prendre sont en fonction de la sensibilité des données traitées et des risques qui pèsent sur les personnes en cas d'incident.

En pratique, rapprochez-vous de votre prestataire informatique pour vérifier avec lui que vos antivirus et logiciel sont à jour et que vos mots de passe sont changés suffisamment régulièrement. La CNIL a édité un guide très complet à ce sujet : Le guide sur la sécurité des données personnelles

IV- Le délégué à la protection des données (DPD ou DPO)

Les missions du DPD ont été précisées dans des lignes directrices adoptées par le groupe de travail européen constitué par les autorités compétentes en la matière des différents états membres (G29).

Le DPD devra :

- Informer et conseiller le Directeur général en sa qualité de responsable de traitement ;
- Contrôler le respect du règlement et du droit national en matière de protection des données (loi du 6 janvier 1978 I&L) ;
- Conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- Coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci ;
- Tenir compte, dans l'accomplissement des missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Sa désignation est requise dans trois cas :

- Lorsque le traitement est effectué par une autorité publique ou un organisme public ;
- Lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitements qui exigent un suivi régulier et systématique à grande échelle des personnes concernées ;
- Lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.

La CNIL a indiqué à l'Union sociale pour l'habitat qu'elle invitait les organismes Hlm à se préparer à la mise en conformité au regard du RGPD et qu'elle préconisait la désignation des DPD.

Les DPD ne sont pas personnellement responsables en cas de non-respect du RGPD. Ce dernier établit clairement que c'est le responsable du traitement ou le sous-traitant qui est tenu de s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément à ses dispositions. Le respect de la protection des données relève de la responsabilité du responsable du traitement ou du sous-traitant.

Le DPD doit pouvoir agir en toute indépendance et ne pas avoir de conflit d'intérêts entre les missions qui peuvent lui être confiées et celle de DPD. Cela signifie en particulier que le DPD ne peut exercer au sein de l'organisme une fonction qui l'amène à déterminer les finalités et les moyens du traitement de données à caractère personnel. En raison de la structure organisationnelle spécifique de chaque organisme, cet aspect doit être étudié au cas par cas.

En pratique : pour les coopératives ayant du patrimoine social, il est très recommandé de désigner un DPD. Si la CNIL n'a pas été explicite pour celles n'exerçant qu'une activité d'accession sociale à la propriété, la désignation d'un DPD est aussi préconisée.

V- Des exemples

A) Le registre de traitements

Pour faciliter la tenue du registre, la CNIL propose **un modèle de registre de base** destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures. Les exemples proposés utilisent la trame du modèle de la CNIL (la trame est en bleu).

Composition du document

1. Une première page du registre recense les informations communes à toutes vos activités de traitement.
2. Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre.

- Les coordonnées de votre coopérative
- Les coordonnées du délégué à la protection des données (DPP) si vous en disposez
- La liste des activités de votre organisme impliquant le traitement de données personnelles.

Première page du registre

Registre des activités de traitement de [Coopérative] Coordonnées du responsable de l'organisme *(Madame Dupont)*	*Ex : Dupont Laurence* *14 rue Lord Byron* *75008 Paris* *0140757948* *Fédération.coop*
Nom et coordonnées du délégué à la protection des données *(Monsieur Durand)*	*Ex : Durand Pierre* *14 rue Lord Byron* *75008 Paris* *0140757948* *Fédération.coop*

Activités de la coopérative impliquant le traitement de données personnelles

Activités	Désignation des activités
Activité 1	*Gestion des prospects*
Activité 2	*Gestion des clients*
Activité 3	*Gestion des coopérateurs*
Activité 4	*Gestion des fournisseurs*
Activité 5	*Gestion des salariés*

Fiche de registre d'activité 1 Fichier des prospects

Date de la création de la fiche		01/01/2010
Date de la dernière mise à jour de la fiche		30/03/2018
Nom du responsable conjoint du traitement (dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)		
Nom du logiciel ou de l'application		Excel

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités

Le traitement a pour objectifs d'effectuer des opérations relatives à la prospection, d'élaborer des statistiques commerciales, d'organisation d'opération promotionnelle.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données

Les personnes concernées sont des prospects

Catégories de données collectées

Listez les différentes données traitées

- ● *Etat-civil, identité, données d'identification, images (nom, prénom, adresse, date et lieu de naissance, etc.)*

  Nom, prénom, civilité, adresse
- ○ *Vie personnelle (habitudes de vie, situation familiale, etc.)*

  Données non collectées
- ○ *Vie professionnelle (CV, situation professionnelles, scolarité, formation, distinctions, diplômes, etc.)*

  Données non collectées
- ○ Informations d'ordre économique et financier (revenus, situation financière, données bancaires, etc.)

  Données non collectées
- ○ Données de connexion (adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)

  Mail
- ○ Données de localisation (déplacements, données GPS, GSM, …)

  Téléphone
- ○ Internet (cookies, traceurs, données de navigation, mesures d'audience, …)

  Données non collectées
- ○ Autres catégories de données (précisez) :

  Non

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

○ Oui ● Non

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

	○ jours	○ mois	○ ans

Autre durée :

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).

Les données sont effacées lorsque la personne est devenue cliente. Sinon elles sont conservées 3 ans maximum à compter de leur collecte. Au terme de ce délai de trois ans, le responsable de traitement prendra contact avec la personne concernée afin de savoir si elle souhaite continuer de recevoir des sollicitations commerciales. En absence de réponse positive et explicite de la personne, les données seront supprimées.[6]

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

1. Service administratif 2. ……

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. …… 2. ……

Sous-traitants

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

1. Prestataire communication 2. Prestataire commercialisateur

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

○	Oui	●	Non

[6] Conformément à la Normes NS48 de la CNIL en attendant la production de référentiels RGPD.

Si oui, vers quel(s) pays :

……..……..……..

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

Contrôle d'accès des utilisateurs

Décrivez les mesures :

Le fichier prospects est enregistré sur un réseau informatique sécurisé. Une procédure permet la gestion sécurisée des demandes d'accès au répertoire général de la coopérative

Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs),* les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

Les données ne sont pas tracées

Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

Les ordinateurs de la coopérative sont dotés d'antivirus régulièrement mis à jour.

Fiche de registre d'activité 2 Fichier des clients

Date de la création de la fiche	01/01/2010
Date de la dernière mise à jour de la fiche	30/03/2018
Nom du responsable conjoint du traitement (dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)	
Nom du logiciel ou de l'application	Excel

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités

Le traitement du fichier client a pour objectifs :

- D'effectuer les opérations relatives à la gestion des clients (les contrats et les actes notariés ; les commandes; les appels de fond ou de redevance; les factures ; la comptabilité; le choix des options et des travaux modificatifs, le suivi de la relation client tel que la réalisation d'enquêtes de satisfaction, la gestion des réclamations et du service après-vente ; la livraison et la levée des réserves, la garantie décennale et la sécurisation Hlm…)
- D'élaborer de statistiques commerciales ;
- De gérer des demandes de droit d'accès, de rectification et d'opposition ;
- de gérer des impayés et du contentieux.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données

Les personnes concernées sont des clients

Catégories de données collectées

Listez les différentes données traitées

- [x] *Etat-civil, identité, données d'identification, images (nom, prénom, adresse, date et lieu de naissance, etc.)*

  Nom, prénom, civilité, adresse pour pouvoir contacter les clients jusqu'à la fin de l'engagement de sécurisation

- [ ] *Vie personnelle (habitudes de vie, situation familiale, etc.)*

  La situation familiale, la composition familiale, la catégorie sociale et professionnlle pour répondre aux enquêtes fédérales

- [ ] *Vie professionnelle (CV, situation professionnelles, scolarité, formation, distinctions, diplômes, etc.)*

  Données non collectées

- [ ] Informations d'ordre économique et financier (revenus, situation financière, données bancaires, etc.)

  Le revenu fiscal N-2 pour vérifier les plafonds de ressources du ménage.

- [ ] Données de connexion (adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)

  Mail

- [ ] Données de localisation (déplacements, données GPS, GSM, …)

  Téléphone

- [ ] Internet (cookies, traceurs, données de navigation, mesures d'audience, …)

  Données non collectées

- [ ] Autres catégories de données (précisez) :

  Non

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

- [ ] Oui
- [x] Non

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

○ jours ○ mois ○ ans

Autre durée :

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).

Les données sont conservées 15 ans pour pouvoir répondre à l'engagement contractuel de sécurisation HLM.

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

1. Service administratif 2. Service financier .....

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. ..... 2. .....

Sous-traitants

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

1. ..... 2. .....

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

○ Oui ● Non

Si oui, vers quel(s) pays :

.....

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

Contrôle d'accès des utilisateurs

Décrivez les mesures :

Le fichier clients est enregistré sur un réseau informatique sécurisé. Une procédure permet la gestion sécurisée des demandes d'accès au répertoire général de la coopérative

Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs)*, les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

Les données ne sont pas tracées

Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

Les ordinateurs de la coopérative sont dotés d'antivirus régulièrement mis à jour.

Fiche de registre d'activité 3 Fichier des coopérateurs

Date de la création de la fiche	01/01/2010
Date de la dernière mise à jour de la fiche	30/03/2018
Nom du responsable conjoint du traitement (dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)	
Nom du logiciel ou de l'application	Excel

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités

Le traitement a pour objectifs de convoquer les coopérateurs aux instances de gouvernance de la coopérative (Assemblée générale, conseil d'administration, commissions…) et de les associer aux actions entreprises pour développer le fait coopératif.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données

Les personnes concernées sont les coopérateurs de la coopérative

Catégories de données collectées

Listez les différentes données traitées

- [x] *Etat-civil, identité, données d'identification, images (nom, prénom, adresse, date et lieu de naissance, etc.)*

  Nom, prénom, civilité, adresse pour convoquer et/ou inviter les coopérateurs
- [ ] *Vie personnelle (habitudes de vie, situation familiale, etc.)*

  Données non collectées
- [ ] *Vie professionnelle (CV, situation professionnelles, scolarité, formation, distinctions, diplômes, etc.)*

  Données non collectées
- [ ] Informations d'ordre économique et financier (revenus, situation financière, données bancaires, etc.)

  Nombre de parts sociales détenues pour calculer les droits de vote à l'assemblée générale

  Montant de part sociale pour calculer le capital social
- [ ] Données de connexion (adresses Ip, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)

  Mail pour convoquer et/ou inviter les coopérateurs

○ Données de localisation (déplacements, données GPS, GSM, …)

Téléphone pour inviter les coopérateurs

○ Internet (cookies, traceurs, données de navigation, mesures d'audience, …)

Données non collectées

○ Autres catégories de données (précisez) :

Non

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

○ Oui ● Non

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

	○ jours	○ mois	○ ans

Autre durée :

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).

Les données sont conservées tant que le coopérateur détient des parts sociales de la coopérative. Elles sont effacées 5 ans après le remboursement des parts sociales au coopérateur.

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

1. Service administratif 2. Service financier……

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. …… 2. ……

Sous-traitants

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

1. Prestataire communication 2. ……

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

○	Oui	●	Non

Si oui, vers quel(s) pays :

……..……..……..

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

Contrôle d'accès des utilisateurs

Décrivez les mesures :

Le fichier coopérateurs est enregistré sur un réseau informatique sécurisé. Une procédure permet la gestion sécurisée des demandes d'accès au répertoire général de la coopérative

Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs),* les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

Les données ne sont pas tracées

Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

Les ordinateurs de la coopérative sont dotés d'antivirus régulièrement mis à jour.

B) Des mentions

Exemple de mention pour la collecte des données clients (générée sur le site de la CNIL).

Les informations recueillies sur ce formulaire sont enregistrées dans un fichier informatisé par **COOPERATIVE** pour **la gestion de la clientèle.**

Elles sont conservées pendant **15 ans** et sont destinées **aux services administratif, financier et communication de la coopérative.**

Conformément à la loi « informatique et libertés », vous pouvez exercer votre droit d'accès aux données vous concernant et les faire rectifier en contactant : **Le service administratif, adresse mail.**

Nous vous informons de l'existence de la liste d'opposition au démarchage téléphonique « Bloctel », sur laquelle vous pouvez vous inscrire ici : https://conso.bloctel.fr/

Exemple de mention pour les formulaires d'enquête OPS

(Cahier repère 41 Union sociale pour l'Habitat)

Identité et coordonnées du responsable de traitement : Organisme XXX

Coordonnées du CIL ou DPO (le cas échéant) : XXXXX

Conformément à l'article L 442-5 du code de l'habitat et de la construction, l'organisme d'habitations à loyer modéré, XXXX, traite les données à caractère personnel recueillies à l'occasion des enquêtes mentionnées au premier alinéa du présent article en vue de créer des outils d'analyse de l'occupation sociale de leur parc contribuant au système de qualification de

l'offre mentionné à l'article L. 441-2-8, à l'élaboration et à la mise en œuvre des orientations en matière d'attributions de logements mentionnées à l'article L. 441-1-5, à l'élaboration des conventions d'utilité sociale prévues à l'article L. 445-1 et du programme local de l'habitat mentionné à l'article L. 302-1, ainsi qu'à l'identification des ménages en situation de précarité énergétique pour l'application de l'article L. 221-1-1 du code de l'énergie.

L'organisme XXX est autorisé à transmettre les données recueillies rendues anonymes au représentant de l'Etat dans le département et dans la région, à la région, au département, aux établissements publics de coopération intercommunale mentionnés au vingtième alinéa de l'article L. 441-1, aux établissements publics territoriaux de la métropole du Grand Paris (à supprimer le cas échéant), à la métropole de Lyon (à supprimer le cas échéant), aux communes ainsi qu'à l'Union sociale pour l'habitat regroupant les fédérations d'organismes d'habitations à loyer modéré, aux dites fédérations et aux associations régionales d'organismes d'habitations à loyer modéré, à la fédération des entreprises publiques locales, à la société mentionnée à l'article L. 313-191, au groupement d'intérêt public mentionné à l'article L. 441-2-12, ainsi qu'aux agences d'urbanisme dès lors que ces agences interviennent dans le cadre d'une étude définie en relation avec une collectivité territoriale ou un groupement de collectivités territoriales. » (article L 442-5 du CCH).

1 Action Logement

2 GIP SNE

Les catégories de données traitées sont celles contenues dans l'arrêté du XXXXX.

Les locataires sont tenus de répondre dans le délai d'un mois. A défaut, le locataire défaillant est redevable à l'organisme d'habitations à loyer modéré d'une pénalité de 7,62 euros, majorée de 7,62 euros par mois entier de retard, sauf s'il est établi que des difficultés particulières n'ont pas permis au locataire de répondre.

Tout locataire dispose d'un droit d'accès et de rectification.

Les formulaires d'enquêtes sont conservés jusqu'au renouvellement de l'enquête, soit deux ans pour l'enquête OPS.

VI- Annexes

A) Des ressources complémentaires

- Le site de la CNIL : https://www.cnil.fr/professionnel
- Le lien pour générer des mentions : https://www.cnil.fr/fr/modeles/mention
- Le guide sur la sécurité des données personnelles : https://www.cnil.fr/fr/un-nouveau-guide-de-la-securite-des-donnees-personnelles
- Le guide pratique pour les sous-traitants : https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants
- L'outil de la CNIL pour générer des mentions : https://www.cnil.fr/modeles/mention
- Le réseau informatique et libertés de l'Union sociale pour l'habitat : reseauinformatiquelibertes.hlm.union-habitat.org/ush/Main
- Une vidéo bien faite : https://www.comptoir-numerique-hlm.fr/une-presentation-du-rgpd-a-mettre-entre-toutes-les-mains

B) Exemple de lettre de mission pour un DPD (Union sociale pour l'Habitat)

Modèle de lettre de mission pour la nomination d'un délégué (e) à la protection des données

Madame, Monsieur,

Il a été procédé à votre désignation en tant que Délégué à la Protection des Données de l'organisme XXXX.

Cette désignation, effectuée en application des articles 37 à 39 du règlement européen relatif à la protection des données 2016/678 du 27 avril 2016 (RGPD), des lignes directrices adoptées par le G 29 le 13 décembre 2016 et de la loi n°78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, est effective à compter du XXX.

Cette désignation fera l'objet dès la mise en ligne du formulaire par la CNIL (ou a fait l'objet) d'une déclaration à la CNIL en date du XXX.

En application de l'article 38 du RGPD, vous êtes, au titre de cette mission, directement rattaché (e) au directeur (trice) général (e).

Les instances représentatives du personnel ont été préalablement informées de cette nomination en date du XXX.

Vous exercerez cette mission pour l'intégralité des traitements de données comportant des données à caractère personnel mis en oeuvre par l'organisme XXX.

Il vous appartiendra de veiller de manière indépendante au respect de la loi Informatique et liberté et à la mise en oeuvre du RGPD. A ce titre, le directeur général, en sa qualité de responsable de traitement veille à ce que vous ne receviez aucune instruction en ce qui concerne l'exercice de vos missions en tant que délégué à la protection des données (cf article 38 du RGPD).

Je vous rappelle que vous êtes soumis au secret professionnel.

Au titre de votre fonction, vous devrez :

 informer et conseiller le directeur général en sa qualité de responsable de traitement ;

 contrôler le respect du règlement et du droit national en matière de protection des données (loi du 6 janvier 1978 I&L);

 conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;

 coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci ;

 tenir compte, dans l'accomplissement des missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Pour vous permettre de mener à bien ces différentes missions, la direction générale s'engage à :

- vous proposez des formations relatives à la protection des données ;
- vous permettre de mener des actions de communication interne auprès du personnel, par le biais de communiqués, de l'intranet, de brochures, de stages ;
- mettre à votre disposition les moyens matériels suivants : adresse e-mail dédiée, espace dédié dans l'intranet ;
- vous communiquer tous les éléments permettant d'établir et d'actualiser la liste des traitements (registre) ;
- vous consultez préalablement à la mise en oeuvre de tout nouveau traitement.

Une copie de cette lettre de mission sera diffusée à l'ensemble du personnel de l'organisme le XXX.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées. Signature du ou de la délégué (e)

Signature du directeur (trice) général (e) à la protection des données

C) La licéité d'un traitement

La CNIL définit qu'un traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

e) 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;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

Identification de la base légale de traitement pour un bailleur

Cahier Repères numéro 41 de l'Union sociale pour l'habitat

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