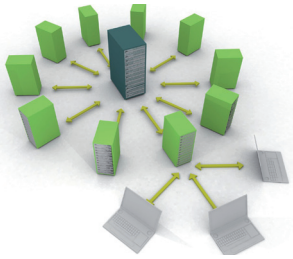
FIEEC

FEDERATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

Juin 2014

Pack de conformité

« *Smart grids* et données personnelles »



Contact : Julie MACAIRE
Responsable des affaires juridiques
Tél : +33 1 45 05 70 52
jmacaire@fieec.fr

CNIL

Commission Nationale de l'Informatique et des Libertés

Sommaire

Isabelle FALQUE-PIERROTIN
Présidente de la CNIL

« *La coopération qui se noue entre la FIEEC et la CNIL est, à mes yeux, exemplaire de l'évolution de notre institution et des besoins nouveaux de régulation que suscite le numérique.*

Dans un monde en mutation, il est en effet nécessaire que la CNIL se rapproche des entreprises et s'ouvre à l'innovation pour accompagner celle-ci.

Elle doit être capable, en outre, de proposer de nouveaux outils de mise en conformité. Afin que ceux-ci soient les plus efficients, la Cnil recherche de nouveaux modes de relation avec les professionnels.

A cet égard, les travaux menés par le groupe de travail mis en place dans le cadre du partenariat entre la CNIL et la FIEEC, sur les smart grids et la protection des données personnelles, démontrent la possibilité d'ouvrir des voies d'innovations durables construites sur la confiance.

On a trop entendu dire que la protection de données était contraire à l'innovation. Le travail effectué avec la FIEEC déconstruit cette idée en montrant qu'assurer la transparence et le contrôle par les personnes de leurs données donne au contraire un avantage concurrentiel aux entreprises.

Ces travaux réalisés en l'espace d'une année sont destinés à être revisités à intervalle régulier pour les adapter aux évolutions technologiques. Par ailleurs, ils seront portés au niveau du groupe des CNIL européennes, dont j'assure la présidence, tant il est vrai que les questions de protection des données viennent percuter les enjeux concurrentiels qui existent actuellement entre les grandes zones du monde.

Enfin, notre partenariat s'est avéré suffisamment utile pour qu'il soit envisagé de poursuivre cette initiative dans d'autres domaines que le pilotage de la gestion énergétique. C'est donc avec énergie et enthousiasme que nous poursuivrons nos travaux avec la FIEEC. »

FIEEC

FEDERATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

Gilles SCHNEPP,
Président de la FIEEC

« *La transition numérique et énergétique de notre société entraine une multiplication des échanges de données, notamment personnelles, dans tous les aspects de la vie quotidienne des citoyens, des entreprises ou des administrations.*

Au cœur de cette évolution majeure, les industries de notre secteur ont une conviction : la confiance dans le numérique est une nécessité pour garantir le développement de nouvelles réponses à ces usages.

Le partenariat mis en œuvre entre la CNIL et la FIEEC il y a plus d'un an, s'inscrit dans cette dynamique et vient répondre au souhait des industriels d'innover dans le strict respect des droits et des libertés individuelles.

Cette approche traduit une volonté commune de mettre en avant une nouvelle vision de la régulation visant à privilégier une démarche positive de « privacy by design ». L'idée est bien d'intégrer la protection des données personnelles en amont de la conception des produits et solutions et d'en faire ainsi un réel levier de compétitivité. L'objectif est ainsi de favoriser l'accompagnement des acteurs en vue d'assurer un haut niveau de protection des citoyens et des consommateurs sans entraver l'innovation des acteurs économiques.

Le résultat de nos premiers travaux portant sur les « smart grids » illustre l'importance des échanges entre les industriels et une autorité de régulation, telle que la Commission Nationale de l'informatique et des libertés.

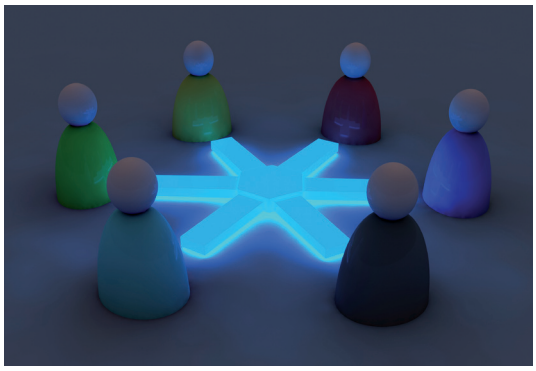
Nous nous félicitons de poursuivre ce partenariat innovant sur de nouveaux sujets qui présentent des enjeux importants pour nos entreprises.

Nous souhaitons adresser nos plus vifs remerciements à la Commission Nationale de l'Informatique et des Libertés pour son engagement fort et constant, ainsi qu'à sa Présidente, Isabelle FALQUE-PIERROTIN, pour son implication personnelle dans ce partenariat ». »

Pourquoi un « pack de conformité » ?

Le pack de conformité est un nouvel outil de régulation des données personnelles qui recouvre tout à la fois :

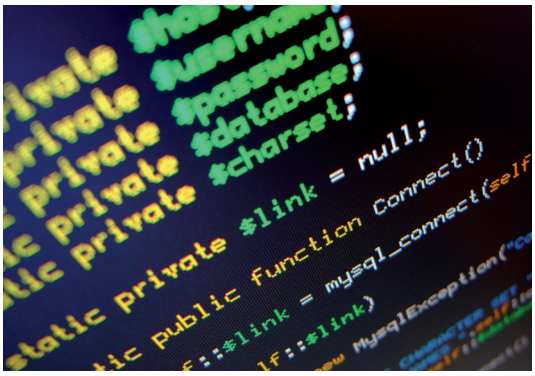
- une méthode de travail basée sur un partenariat étroit entre les représentants du secteur des industries électriques, électroniques et de communicaiton et la CNIL qui permet de faire remonter les bonnes ou mauvaises pratiques, les problèmes rencontrés, les demandes des usagers, les spécificités du secteur concerné et les questions qui se posent sur le terrain.
- un nouveau mode de régulation pour la CNIL : il s'agit de bâtir des référentiels sectoriels, mettant à plat les traitements de données personnelles du secteur pour déboucher sur :
  - ◊ un ensemble de règles et de bonnes pratiques déclinées au moyen des vecteurs juridiques existants tels que normes simplifiées, autorisations uniques, recommandations, reconnaissance de la conformité des règles professionnelles, mais aussi des fiches pratiques élaborées pour clarifier et donner des exemples concrets,
  - ◊ des modes opératoires et processus organisationnels liés à la mise en place de correspondants informatique et libertés, de règles internes d'entreprises (appelés BCR), de labels…



Ce référentiel a un double objectif :

- sécuriser juridiquement les professionnels en donnant des indications concrètes sur la façon de respecter les textes et des modes opératoires précis.
- simplifier les formalités autant que la loi actuelle le permet, en utilisant les dispenses, normes simplifiées et autorisations uniques,

C'est ainsi que dans le cadre du partenariat entre la Commission Nationale de l'Informatique et des Libertés (CNIL) et la Fédération des Industries Électriques, Électroniques et de Communication (FIEEC) engagé en octobre 2012, un groupe de travail a été créé sur les traitements de données personnelles relatives à la consommation électrique collectées par les appareils installés par les usagers, hors de l'infrastructure des compteurs communicants déployés par les gestionnaires de réseau.



La création du groupe de travail CNIL / FIEEC

En octobre 2012,à l'issue d'une matinée - débat, la FIEEC et la CNIL ont fait le constat commun de la nécessité de travailler ensemble sur le sujet majeur des données personnelles. Afin de lancer ce partenariat très concrètement, un premier sujet a été choisi pour être approfondi par un groupe de travail ad hoc dénommé « *Smart grids* et protection des données personnelles ».

Ce groupe de travail avait pour objectif d'aboutir à la publication de **« scénario d'innovation »** relatifs aux questions de collecte et de traitement des données personnelles relatives à la consommation électrique par les appareils installés par les usagers en « aval des compteurs électriques » (par exemple, directement sur le tableau électrique ou via une prise sur le compteur permettant de collecter des données de consommation précises).

L'objectif de ce groupe de travail était d'aboutir à la publication de bonnes pratiques visant à accompagner l'innovation des industriels du secteur en intégrant la protection des données personnelles le plus en amont possible dans la définition des nouveaux services, « privacy by design ».

Ces travaux concernent uniquement les traitements de données collectées via des appareils ou logiciels installés :

- **hors de l'infrastructure des compteurs, c'est-à-dire en aval des compteurs** sont donc exclus des présents travaux les traitements de données réalisés directement via les compteurs électriques ;
- à la demande et sous la maîtrise des particuliers pour leur fournir des services spécifiques (B to C).

Afin de faciliter la mise en conformité de ces dispositifs à la loi Informatique et Libertés, **trois hypothèses de travail** ont été dégagées, correspondant aux trois scenarios pouvant être rencontrés par les professionnels du secteur. S'adressant à des professionnels, ces lignes directrices permettent pour chaque type de traitement identifié, de préciser leurs finalités, les catégories de données collectées, leur durée de conservation, les droits des personnes, les mesures de sécurité à mettre en place et les destinataires des informations.

Elles ont vocation à être portées au niveau européen, tant par la FIEEC que par la CNIL, pour permettre aux acteurs de se positionner sur un marché européen sinon mondial, faisant de la protection des données un facteur de compétitivité.

La démarche de travail est avant tout centrée sur l'usager, ce qui constitue un facteur de confiance déterminant pour les consommateurs afin qu'ils fassent le choix de ces produits innovants.

Ces lignes directrices sont représentatives de l'appréhension à un moment donné des technologies et usages associés et feront l'objet d'un bilan annuel. Leur caractère souple et évolutif doit donc être souligné.

Périmètre des 3 schémas d'innovation

Scénario 1
IN - IN

La gestion des données collectées dans le logement sans communication vers l'extérieur.

Dans ce scenario, les données collectées dans le logement restent sous la maîtrise unique de l'usager et ne sont pas destinées à être collectées ou réutilisées par un tiers, ce qui peut correspondre à deux cas :

1. Les applications purement « IN-IN » : plusieurs produits ou solutions communiquent entre eux sans sortie de données vers l'extérieur.
2. Les applications qui impliquent une sortie des données du logement sans que ces données ne soient transmises pour réutilisation à des tiers. Sont ainsi concernées les applications pour lesquelles les données :
   - restent confinées sur des réseaux de communications intégralement sous la maitrise de l'usager (type Wifi ou autre réseau local) ;
   - circulent sur des réseaux de télécommunications ouverts au public (type ADSL, fibre, GSM).

Scénario 3
IN - OUT - IN

La gestion des données collectées dans le logement et transmises à l'extérieur pour permettre un pilotage à distance de certains équipements du logement.

Dans ce scénario, les données :

- sortent du logement pour être transmises à un ou des prestataires, que cette sortie soit matériellement effectuée par la personne ou par le prestataire lui-même ;
- sont traitées par le prestataire pour proposer un service à la personne impliquant une interaction avec le logement dans un objectif de pilotage énergétique des équipements du logement.

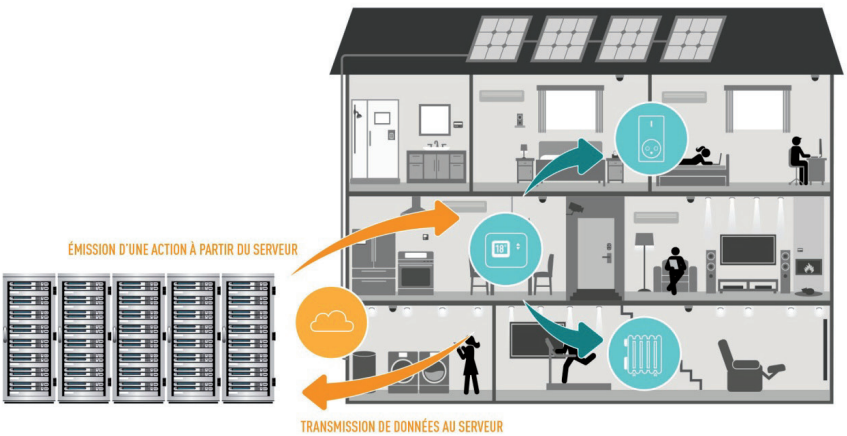
La gestion des données collectées dans le logement et transmises à l'extérieur.

Dans ce scenario, les données collectées :

- sortent du logement pour être transmises à un ou des prestataires, que cette sortie soit matériellement effectuée par la personne ou par le prestataire lui-même ;
- sont traitées par le prestataire pour proposer un service à la personne sans pour autant déclencher une action dans le logement.

Scénario 2

IN - OUT



Fiche 1 - Scénario « IN - IN » :
La gestion des données collectées dans le logement sans communication vers l'extérieur

Périmètre

Dans ce scenario, les données collectées dans le logement restent sous la maîtrise unique de l'usager et ne sont pas destinées à être réutilisées par un tiers, ce qui peut correspondre à deux cas :

1. **Les applications purement « IN-IN » :** plusieurs produits ou solutions communiquent entre eux à l'intérieur du logement, sans aucune sortie de données vers l'extérieur ;
   Par exemple : communication entre le thermostat et le chauffage, gestion du chauffage zone par zone, mise en veille de la maison au départ de l'occupant, déploiement des volets roulants en fonction du niveau d'ensoleillement ou de la température ambiante dans la zone déterminé par un capteur.

2. **Les applications qui impliquent une sortie des données du logement, sans que ces données ne soient transmises à des tiers.** Sont ainsi concernées les applications pour lesquelles les données :
   - restent confinées sur des réseaux de communications intégralement sous la maîtrise de la personne (type Wifi ou autre réseau local) ;
   - circulent sur des réseaux de télécommunications ouverts au public (type ADSL, fibre, GSM).

   Par exemple : une application smartphone utilisée par la personne qui communique directement avec du matériel installé dans son domicile.

Le fait que les données passent sur les réseaux gérés par des opérateurs de communications électroniques ne pose pas de difficultés dans la mesure où ces opérateurs ont des obligations renforcées quant à ce qu'ils peuvent faire avec ces données de trafic. Ceci n'est cependant valable que si l'opérateur en question agit bien en tant que fournisseur du service de communication électronique. A l'inverse, si l'opérateur souhaite fournir un autre service, les recommandations applicables sont celles des fiches 2 ou 3.

Analyse au regard de la loi Informatique et Libertés

La mise en place d'un traitement de données personnelles doit respecter la loi Informatique et Libertés. En effet, toute personne qui souhaite traiter des données personnelles est soumise à un certain nombre d'obligations légales, sauf dans le cas des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, ce qui est le cas dans le scenario présenté dans cette fiche.

Dans la mesure où dans ce scenario les dispositifs restent sous la maîtrise unique de la personne, la principale problématique s'avère être celle de la sécurité des données.

Finalités poursuivies par les traitements

- **Finalité 1 : gestion des équipements et information sur la consommation :** la personne souhaite obtenir des informations sur sa consommation d'énergie ou faire communiquer plusieurs appareils de son logement afin d'obtenir des services de domotique ou d'efficacité énergétique. Elle installe pour cela un ou plusieurs produits (un écosystème) ;
- **Finalité 2 : information sur la consommation dans les logements neufs au titre de la Réglementation Thermique 2012 (RT 2012) :** l'occupant du logement est informé sur sa consommation d'énergie au moyen d'appareils installés dans son logement.

Base légale : la base légale du traitement est le consentement de la personne

- Pour la finalité 1, le recueil de ce consentement se fera lors de la souscription du contrat par la personne concernée auprès d'un prestataire pour que ce dernier lui fournisse un service déterminé. Le consentement sera donc recueilli au moment de la signature du contrat ;
- Pour la finalité 2, l'occupant du logement doit pouvoir maîtriser le système. Ainsi, il doit être en mesure de pouvoir désactiver lui-même le système ou pouvoir en faire la demande. En effet, la RT 2012 impose au propriétaire/bailleur d'installer un appareil dans le logement permettant d'informer l'occupant sur sa consommation, mais ce dernier peut ne pas souhaiter bénéficier de cette information.

Le consentement doit être une manifestation de volonté libre, spécifique et informée de la personne à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement (par exemple, case à cocher non pré-cochée, branchement d'un produit dans le logement).

Données collectées

Seules peuvent être collectées les données personnelles nécessaires à la finalité poursuivie par le traitement. Dans le cas d'un contrat de prestation de service souscrit par la personne, les seules données pouvant être collectées sont celles qui sont indispensables à la fourniture du service en question.

Durée de conservation

La durée de conservation des données collectées est déterminée par la personne elle-même puisqu'elle maîtrise le système.

Ainsi, la personne doit être en mesure de supprimer les données personnelles collectées par les dispositifs installés dans son logement, et ce à tout moment (et notamment lorsque la personne déménage ou qu'est requise une opération de service après vente impliquant qu'un tiers puisse avoir accès aux données : mise à jour, réparation…). Cette suppression peut s'effectuer au moyen d'un système prévu dans le dispositif lui-même (bouton, débranchement…) ou par tout autre moyen mis à disposition de la personne.

En tout état de cause, lorsque le prestataire récupère un dispositif qui n'a pas vocation à être réinstallé chez la personne, il doit systématiquement supprimer les données contenues dans ce dispositif. Alors qu'une telle suppression des données est indispensable pour les produits reconditionnables, elle peut s'opérer par la destruction du dispositif lui-même pour les produits en fin de vie.

Destinataires

Dans la mesure où dans ce scenario il n'y a pas de communications vers l'extérieur, la personne concernée peut seule avoir accès aux données.

Information et droits des personnes

Dans la mesure où les traitements sont mis en œuvre pour l'exercice d'activités exclusivement personnelles, il n'y a pas d'obligation d'informer la personne quant à ces traitements.

Cependant, pour la finalité 2 (appareils installés dans le logement au titre de la RT 2012), la personne doit être informée de la présence des ces dispositifs et des moyens pour les désactiver. De même, dès lors que ces appareils permettent de collecter d'autres données que celles prévues réglementairement, il est nécessaire d'en informer spécifiquement la personne et de lui permettre de désactiver cette partie du dispositif.

En outre, le prestataire doit mener une étude d'impact sur la possibilité pour les personnes :

- d'obtenir une copie des données dans un format électronique couramment utilisé et permettant la réutilisation des données,
- de transmettre ces données à un autre système dans un format électronique couramment utilisé.

Sécurité

Le prestataire doit mettre en place des mesures permettant de garantir la sécurité et la confidentialité des données traitées par les appareils qu'il fournit à la personne, et doit prendre toutes les précautions utiles pour en empêcher la prise de contrôle par toute personne non autorisée, notamment en :

- chiffrant tous les échanges de données avec des algorithmes à l'état de l'art,
- protégeant les clés de chiffrement de toute divulgation accidentelle,
- authentifiant les appareils destinataires des données,
- subordonnant l'accès aux fonctionnalités de contrôle de l'installation à une authentification fiable de l'utilisateur (mot de passe, certificat électronique, …).

Les mesures ainsi mises en place doivent être adaptées au niveau de sensibilité des données et aux capacités de contrôle des appareils.

Formalités préalables

Dans la mesure où les traitements sont mis en œuvre pour l'exercice d'activités exclusivement personnelles, il n'y a pas de formalités à effectuer auprès de la CNIL.

Fiche 2 -Scénario - « IN - OUT » :

La gestion des données collectées dans le logement et transmises à l'extérieur

Périmètre

Ce scénario couvre les cas dans lesquels les données :

- sortent du logement pour être transmises à un ou des prestataires, que cette sortie soit matériellement effectuée par la personne ou par le prestataire lui-même ;
- sont traitées par le prestataire pour proposer un service à la personne sans pour autant déclencher une action dans le logement.

Par exemple : proposition par un prestataire d'un nouveau contrat électrique après analyse des consommations.

En pratique, les données peuvent être collectées et traitées par le prestataire qui a conclu directement le contrat avec la personne ou par d'autres tiers à qui ce prestataire a confié la réalisation de tout ou partie de la prestation (les sous-traitants) ou transmis des données (partenaires commerciaux).

Analyse au regard de la loi Informatique et Libertés

La mise en place d'un traitement de données personnelles doit respecter la loi Informatique et Libertés. En effet, toute personne qui souhaite traiter des données personnelles est soumise à un certain nombre d'obligations légales.

Finalités poursuivies par les traitements (liste non exhaustive) :

- **Finalité 1 : suivi de la consommation du logement :** la personne contracte avec un prestataire qui lui fournit un service d'information sur sa consommation. Dans ce cas, les données de consommation sont transmises au prestataire pour être traitées et/ou hébergées, puis mises à disposition de la personne via un affichage déporté ou une plateforme spécifique ;
- **Finalité 2 : réalisation de bilans énergétiques :** la personne contracte avec un prestataire qui analyse ses données de consommation et lui fournit un bilan de sa consommation pour lui proposer des travaux d'isolation, de nouveaux équipements moins énergivores, etc ;
- **Finalité 3 : suivi de la consommation par les bailleurs sociaux :** les bailleurs sociaux accèdent aux données de consommation afin d'aider le locataire à réduire sa consommation d'énergie;
- **Finalité 4 : prospection commerciale :** le prestataire utilise les données personnelles de la personne pour procéder à des opérations de prospection commerciale pour son compte ;
- **Finalité 5 : optimisation des modèles :** un prestataire ou un bailleur social utilise les données de consommation de la personne pour établir des statistiques (données anonymisées ou agrégées ne permettant pas l'identification d'une personne physique).

Base légale

Pour les finalités 1 à 3, la base légale du traitement est le consentement de la personne :

- Pour les finalités 1 et 2 (suivi de la consommation et réalisation de bilan énergétique), le recueil de ce consentement sera recueilli lors de la souscription du contrat par la personne concernée auprès d'un prestataire pour que ce dernier lui fournisse un service déterminé. Le consentement sera donc recueilli au moment de la signature du contrat ;
- Pour la finalité 3 (suivi de la consommation par les bailleurs sociaux), les bailleurs sociaux ne peuvent de droit accéder aux données de consommation du locataire, ils doivent donc obtenir le consentement de ce dernier. Ils peuvent cependant accéder librement aux données anonymisées de l'immeuble ;
- Pour la finalité 4 (prospection commerciale), le prestataire peut librement utiliser les données de la personne (son client) qui sont strictement nécessaires à la réalisation des opérations de prospection commerciale, sauf opposition de celle-ci. En revanche, la CNIL recommande de recueillir systématiquement le consentement de la personne avant toute transmission des données à un autre prestataire.
- Pour la finalité 5 (optimisation des modèles), dans la mesure où les données anonymisées ne sont pas des données personnelles, elles peuvent être librement utilisées.

Pour mémoire, le consentement doit être une manifestation de volonté libre, spécifique et informée de la personne à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement (par exemple, case à cocher non pré-cochée, branchement d'un produit dans le logement).

Données collectées

Seules peuvent être collectées les données personnelles nécessaires à la finalité poursuivie par le traitement. Dans le cas d'un contrat de prestation de service souscrit par la personne, les seules données pouvant être collectées sont celles qui sont indispensables à la fourniture du service en question.

Durée de conservation

- Pour les finalités 1 et 2 (nécessitant la conclusion d'un contrat de prestation de service), il convient de distinguer deux types de données :
  - ◊ **Les données commerciales** (identité de la personne, données relatives aux transactions, aux moyens de paiement…) : ces données peuvent être conservées pendant toute la durée du contrat.

    A l'issue du contrat, elles peuvent faire l'objet d'un archivage physique (sur support distinct : CD-ROM, etc.) ou logique (par gestion des habilitations) pour prévenir d'éventuels contentieux. Puis, à l'issue des durées de prescription légale, les données doivent être supprimées ou anonymisées.

◊ **Les données de consommation** proprement dites : ces données doivent être conservées pendant une durée proportionnée par rapport à la finalité poursuivie :

➲ Lorsque le contrat est conclu pour une durée déterminée (prestation « one shot ») : les données de consommation peuvent être conservées pendant toute la durée du contrat.

Par exemple, pour la finalité 2 (bilan énergétique), les données peuvent être conservées jusqu'à la fourniture à la personne du résultat de l'analyse.

➲ Lorsque le contrat est conclu pour une durée indéterminée : les données peuvent être conservées pendant une durée limitée sous forme détaillée, puis doivent être agrégées pour le reste de la durée du contrat.

Par exemple, pour la finalité 1 (suivi de la consommation), il semble raisonnable de pouvoir conserver les données détaillées pendant trois ans, avant agrégation.

A l'issue du contrat, dans la mesure où les données de consommation détaillées et agrégées ne servent pas à la facturation du service, elles doivent être supprimées ou anonymisées.

- Pour la finalité 3 (suivi de la consommation par les bailleurs sociaux) : les données peuvent être conservées pendant un an sous forme détaillée, puis doivent être agrégées pour le reste de la durée du bail.
- Pour la finalité 4 (prospection commerciale) : les données collectées et conservées au titre des finalités 1 et 2, lorsqu'elles sont strictement nécessaires à la réalisation d'opérations de prospection commerciale, peuvent être conservées par le prestataire pendant un délai de trois ans à compter de la fin de la relation commerciale ;
- Pour la finalité 5 (optimisation des modèles) : dans la mesure où les données anonymisées ne sont pas des données personnelles, elles peuvent être conservées pendant une durée illimitée.

Destinataires

En principe, peuvent seuls avoir accès aux données le prestataire et la personne concernée. Cependant, le prestataire peut être amené à transmettre les données de la personne à un sous-traitant ou à un partenaire commercial.

- **Transmission des données à un sous-traitant :** le prestataire peut librement transmettre des données personnelles à un sous-traitant, auquel il fait appel pour participer à l'exécution du service proposé à la personne.

  Dans cette hypothèse, le prestataire, en tant que responsable de traitement, reste responsable des conditions de traitement des données par son sous-traitant. De son côté, le sous-traitant a pour seule obligation d'assurer la sécurité et la confidentialité des données.

- **Transmission des données à un partenaire commercial :**
  - Si les données transmises sont des données anonymes (notamment finalité 5): le prestataire peut librement transmettre les données à un partenaire commercial. Ni le prestataire, ni le partenaire commercial n'ont alors d'obligation au regard de la loi Informatique et Libertés, celle-ci étant pas applicable aux données anonymes ;
  - Si les données transmises sont des données personnelles :
    - ➲ Pour les finalités 1 à 3, le prestataire doit recueillir le consentement de la personne avant toute transmission de ses données au partenaire commercial (par exemple, via une case à cocher non pré-cochée ou, lorsque cela est techniquement possible, via un dispositif physique ou logique accessible du logement par la personne) ;
    - ➲ Pour la finalité 4 (prospection commerciale), la CNIL recommande de recueillir systématiquement le consentement de la personne.

      Dans les deux cas, le partenaire commercial devient à son tour responsable de traite-

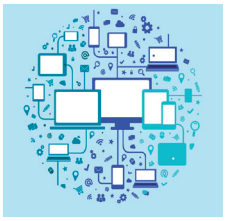
ment pour le traitement des données qui lui sont transmises et est soumis à l'ensemble des dispositions de la loi Informatique et Libertés.

Information et droits des personnes

la personne doit être informée, préalablement à la mise en œuvre du traitement, de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, ainsi que des droits dont elle dispose au titre de la loi Informatique et Libertés. Cette information pourrait être effectuée lors de la signature du contrat de prestation de service par la personne concernée.

Par ailleurs, la personne dispose d'un droit d'accès, de rectification et de suppression de ses données. Le prestataire doit permettre à la personne d'exercer son droit d'accès de la façon la plus efficace possible, sachant que l'intégralité des données personnelles que détient le prestataire est concernée par ce droit.

Pour les finalités 1 à 3, la personne peut également retirer son consentement en résiliant le contrat qu'elle a conclu avec le prestataire, ce qui doit conduire à l'arrêt du traitement. Les données doivent alors être supprimées, anonymisées ou archivées. Pour la finalité 4 (prospection commerciale), la personne doit être mise en mesure de s'opposer, sans frais, au traitement de ses données par le prestataire. Pour la finalité 5 (optimisation des modèles), dans la mesure où les données anonymisées ne sont pas des données personnelles, les personnes n'ont pas à être informées.



En outre, le prestataire doit mener une étude d'impact sur la possibilité pour les personnes :

- d'obtenir une copie des données dans un format électronique couramment utilisé et permettant la réutilisation des données ;
- de transmettre ces données à un autre système dans un format électronique couramment utilisé.

Sécurité

le prestataire doit mettre en place des mesures permettant de garantir la sécurité et la confidentialité des données traitées par les appareils qu'il fournit à la personne, et doit prendre toutes les précautions utiles pour en empêcher la prise de contrôle par une personne non autorisée, notamment en :

- chiffrant tous les échanges de données avec des algorithmes à l'état de l'art,
- protégeant les clés de chiffrement de toute divulgation accidentelle,
- authentifiant les appareils destinataires des données,
- subordonnant l'accès aux fonctionnalités de contrôle de l'installation à une authentification fiable de l'utilisateur (mot de passe, certificat électronique, …).

Les mesures ainsi mises en place doivent être adaptées au niveau de sensibilité des données.

Concernant les mesures à mettre en place au niveau des infrastructures externes au logement, le prestataire doit mener une étude des risques engendrés par le traitement afin de déterminer et de mettre en œuvre les mesures nécessaires à la protection de la vie privée des personnes. La CNIL met à disposition une méthode de ce type sur son site web (www.cnil.fr/les-themes/securite/), mais d'autres méthodes équivalentes peuvent être utilisées.

Formalités préalables

Le prestataire doit effectuer une déclaration normale auprès de la CNIL. Cette déclaration doit être effectuée sur le site de la CNIL (www.cnil.fr).

Fiche 3 - Scénario - « IN - OUT - IN » :

La gestion des données collectées dans le logement et transmises à l'extérieur pour permettre un pilotage à distance de certains équipements du logement.

Périmètre

Ce scénario couvre les cas dans lesquels les données :

- sortent du logement pour être transmises à un ou des prestataires, que cette sortie soit matériellement effectuée par la personne ou par le prestataire lui-même ;
- sont traitées par le prestataire pour proposer un service à la personne impliquant une interaction avec le logement dans un objectif de pilotage énergétique des équipements du logement.

Par exemple : service permettant à la personne de commander la production d'eau chaude sanitaire, l'enclenchement de sa pompe à chaleur, le déclenchement de sa machine à laver ou le chargement de son véhicule électrique au moment où l'électricité est la moins chère.

En pratique, les données peuvent être collectées et traitées par le prestataire qui a conclu directement le contrat avec la personne (le prestataire) ou par d'autres prestataires à qui ce prestataire a confié la réalisation de tout ou partie de la prestation (les sous-traitants).

Analyse au regard de la loi Informatique et Libertés

La mise en place d'un traitement de données personnelles doit respecter la loi Informatique et Libertés. En effet, toute personne qui souhaite traiter des données personnelles est soumise à un certain nombre d'obligations légales.

Finalités poursuivies par les traitements (liste non exhaustive) :

- **Finalité 1 : effacement de la consommation du logement :** la personne contracte avec un prestataire qui lui fournit un service d'effacement, permettant d'activer ou de désactiver à distance certains équipements du logement dans certaines situations identifiées et ainsi de décaler leur consommation. Dans ce cas, les données sont transmises au prestataire qui les traite pour déterminer quand il convient d'intervenir sur les équipements du logement (par exemple : service permettant d'éteindre le chauffage au dessus de 19 degrés lors d'un pic de consommation) ;
- **Finalité 2 : efficacité énergétique du logement :** la personne contracte avec un prestataire qui lui fournit un service permettant d'améliorer l'efficacité énergétique de son logement en agissant sur différents équipements du logement. Dans ce cas, des données sont transmises au prestataire qui les traite pour déterminer l'action à mener dans le logement (par exemple : service permettant de fermer les volets en cas d'absence du logement).
- **Finalité 3 : prospection commerciale :** le prestataire utilise les données personnelles de la personne pour procéder à des opérations de prospection commerciale pour son compte.

Base légale

Pour les finalités 1 et 2 (effacement et efficacité énergétique), la base légale du traitement est le consentement de la personne. Le recueil de ce consentement se fera lors de la souscription du contrat par la personne concernée auprès d'un prestataire pour que ce dernier lui fournisse un service déterminé. Le consentement sera donc recueilli au moment de la signature du contrat.

Pour la finalité 3 (prospection commerciale), le prestataire peut librement utiliser les données de la personne (son client) qui sont strictement nécessaires à la réalisation des opérations de prospection commerciale, sauf opposition de celle-ci. En revanche, la CNIL recommande de recueillir systématiquement le consentement de la personne avant toute transmission des données à un autre prestataire.

Le consentement doit être une manifestation de volonté libre, spécifique et informée de la personne à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement (par exemple, case à cocher non pré-cochée, branchement d'un produit dans le logement).

Données collectées

Seules peuvent être collectées les données personnelles nécessaires à la finalité poursuivie par le traitement. Dans le cas d'un contrat de prestation de service souscrit par la personne, les seules données pouvant être collectées sont celles qui sont indispensables à la fourniture du service en question.

Durée de conservation :

- Pour les finalités 1 et 2 (nécessitant la conclusion d'un contrat de prestation de service), il convient de distinguer deux types de données :
  - **Les données commerciales** (identité de la personne, données relatives aux transactions, aux moyens de paiement…) : ces données peuvent être conservées pendant toute la durée du contrat. A l'issue du contrat, elles peuvent faire l'objet d'un archivage physique (sur support distinct : CD-ROM, etc.) ou logique (par gestion des habilitations) pour prévenir d'éventuels contentieux. Puis, à l'issue des durées de prescription légale, les données doivent être supprimées ou anonymisées.
  - **Les données de consommation proprement dites et les données de commande** (données relatives aux demandes d'action sur les équipements du logement et résultats éventuels de ces actions) : ces données doivent être conservées pendant une durée limitée sous forme détaillée, puis doivent être agrégées pour le reste de la durée du contrat.En l'espèce, il semble raisonnable de pouvoir conserver les données détaillées pendant trois ans, avant agrégation.

    A l'issue du contrat, dans la mesure où les données de consommation détaillées et agrégées ne servent pas à la facturation du service, elles doivent être supprimées ou anonymisées.
- Pour la finalité 3 (prospection commerciale) : les données collectées et conservées au titre des finalités 1 et 2, lorsqu'elles sont et strictement nécessaires à la réalisation d'opérations de prospection commerciale, peuvent être conservées par le prestataire pendant un délai de trois ans à compter de la fin de la relation commerciale.

Destinataires

En principe, peuvent seuls avoir accès aux données le prestataire et la personne concernée.

Cependant, le responsable de traitement peut être amené à transmettre les données de la personne à un sous-traitant ou un partenaire commercial.

- **Transmission des données à un sous-traitant :** le prestataire peut librement transmettre des données personnelles à un sous-traitant, auquel il fait appel pour participer à l'exécution du service proposé à la personne.

  Dans cette hypothèse, le prestataire, en tant que responsable de traitement, reste responsable des conditions de traitement des données par son sous-traitant. De son côté, le sous-traitant a pour seule obligation d'assurer la sécurité et la confidentialité des données.
- **Transmission des données à un partenaire commercial :**
  - Si les données transmises sont des données anonymes : le prestataire peut librement transmettre les données à un partenaire commercial. Ni le prestataire, ni le partenaire commercial n'ont alors d'obligation au regard de la loi Informatique et Libertés, celle-ci étant pas applicable aux données anonymes ;
  - Si les données transmises sont des données personnelles :
    - ➲ Pour les finalités 1 et 2, le prestataire doit recueillir le consentement de la personne avant toute transmission de ses données au partenaire commercial (par exemple, via une case à cocher non pré-cochée ou, lorsque cela est techniquement possible, via un dispositif physique ou logique accessible du logement par la personne) ;
    - ➲ Pour la finalité 3 (prospection commerciale), la CNIL recommande de recueillir systématiquement le consentement de la personne.
      Dans les deux cas, le partenaire commercial devient à son tour responsable de traitement pour le traitement des données qui lui sont transmises et est soumis à l'ensemble des dispositions de la loi Informatique et Libertés.

Information et droits des personnes

La personne doit être informée, préalablement à la mise en œuvre du traitement, de l'identité du responsable de traitement, de la finalité du traitement, des destinataires des données, ainsi que des droits dont elle dispose au titre de la loi Informatique et Libertés. Cette information pourrait être effectuée lors de la signature du contrat de prestation de service par la personne concernée.

Par ailleurs, la personne dispose d'un droit d'accès, de rectification et de suppression de ses données. Le prestataire doit permettre à la personne d'exercer son droit d'accès de la façon la plus efficace possible, sachant que l'intégralité des données personnelles que détient le prestataire est concernée par ce droit.

Pour les finalités 1 et 2, la personne peut également retirer son consentement en résiliant le contrat qu'elle a conclu avec le prestataire, ce qui doit conduire à l'arrêt du traitement. Les données doivent alors être supprimées, anonymisées ou archivées. Pour la finalité 3 (prospection commerciale), la personne doit être mise en mesure de s'opposer, sans frais, au traitement de ses données par le prestataire.

Par ailleurs, le prestataire doit prévoir une fonctionnalité de débrayage manuel du dispositif permettant à la personne de contrecarrer les actions menées à distance sur les équipements de son logement (exemple : relancer le chauffage qui a été coupé dans le cadre d'une prestation d'effacement).

Enfin, le prestataire doit mener une étude d'impact sur la possibilité pour les personnes :

- d'obtenir une copie des données dans un format électronique couramment utilisé et permettant la réutilisation des données ;
- de transmettre ces données à un autre système dans un format électronique couramment utilisé.

Sécurité

Le prestataire doit mettre en place des mesures permettant de garantir la sécurité et la confidentialité des données traitées par les appareils qu'il fournit à la personne, et doit prendre toutes précautions utiles pour en empêcher la prise de contrôle par une personne non autorisée, notamment en :

- chiffrant tous les échanges de données avec des algorithmes à l'état de l'art,
- protégeant les clés de chiffrement de toute divulgation accidentelle,
- authentifiant les appareils destinataires des données,
- subordonnant l'accès aux fonctionnalités de contrôle de l'installation à une authentification fiable de l'utilisateur (mot de passe, certificat électronique, …).

Les mesures ainsi mises en place doivent être adaptées au niveau de sensibilité des données et aux capacités de contrôle des appareils.

Concernant les mesures à mettre en place au niveau des infrastructures externes au logement, le prestataire doit mener une étude des risques engendrés par le traitement afin de déterminer et de mettre en œuvre les mesures nécessaires à la protection de la vie privée des personnes. La CNIL met à disposition une méthode de ce type sur son site web (www.cnil.fr/les-themes/securite/), mais d'autres méthodes équivalentes peuvent être utilisées.

Enfin, le prestataire doit développer ses produits et services en intégrant dès l'origine la problématique des données personnelles (*privacy by design*). A tout le moins, le produit ou service doit limiter la sortie du logement des données à ce qui est strictement nécessaire à la fourniture du service, et privilégier les décisions prises localement à celles réalisées à l'extérieur du logement. Le prestataire doit également favoriser une anonymisation des données le plus tôt possible dans la chaine de collecte. Dès lors que les données sont anonymes, il est rappelé que la loi Informatique et Libertés ne s'applique plus et que les données peuvent donc être conservées et échangées de façon illimitée.

Formalités préalables

Le prestataire doit effectuer une déclaration normale auprès de la CNIL. Cette déclaration doit être effectuée sur le site de la CNIL (www.cnil.fr).

Textes applicables

- Loi informatique et libertés du 6 janvier 1978 modifiée ;
- Arrêté du 26 octobre 2010 relatif aux caractéristiques thermiques et aux exigences de performance énergétique des bâtiments nouveaux et des parties nouvelles de bâtiments (notamment son article 23).

Rappel sur la loi Informatique et Libertés

La loi Informatique et Libertés du 6 janvier 1978 modifiée s'applique dès lors qu'il est procédé à un traitement de données à caractère personnel :

- Constitue un traitement de données personnelles toute opération (collecte, enregistrement, conservation, modification, extraction, consultation, utilisation, communication, interconnexion, destruction…) portant sur des données personnelles.
- Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement.
  Ainsi, sont des données personnelles toutes les données qui, seules ou combinées entre elles, peuvent être rattachées à un usager identifié ou identifiable, un client ou un abonné (températures, consommation d'électricité ou de gaz, volume d'eau chaude consommé, état des appareils électriques…). Les données personnelles ne sont donc pas uniquement les données nominatives (nom et prénom).
  En outre, même si les données peuvent concerner en pratique plusieurs personnes appartenant à un même foyer, la CNIL considère que ce sont des données personnelles dans la mesure où elles sont rattachées à une personne physique identifiée (l'abonné).

La mise en place d'un traitement de données personnelles doit respecter la loi Informatique et Libertés. En effet, toute personne qui souhaite traiter des données personnelles est soumise à un certain nombre d'obligations légales (information des personnes quant au traitement mis en place, voire recueil du consentement, mise en place de modalités d'exercice du droit d'accès et de suppression des données, mesures de sécurité, formalités préalables à effectuer auprès de la CNIL …).

La loi Informatique et Libertés ne s'applique pas dans le cas des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles (comme les traitements décrits dans la fiche n°1) ou lorsque les données traitées sont anonymes, c'est-à-dire lorsqu'elles ne peuvent pas être associées directement ou indirectement à une personne physique en isolant un foyer.

Pour déterminer le mécanisme à mettre en place pour obtenir des données anonymes, le prestataire doit s'interroger quant à la possibilité de ré-identifier les personnes à partir des données obtenues. Il est ainsi nécessaire de prendre en considération la volumétrie des données, leur précision, le nombre de personnes concernées, etc. Les mécanismes d'anonymisation doivent donc être définis au cas par cas. A titre d'exemple, l'agrégation des données permettant de reconstituer les courbes de charges issues de dix foyers indépendants ayant le même profil peut être considérée comme anonyme. De la même manière, un profil de consommation moyen réalisé sur la base de la moyenne des courbes de charge est également considéré comme un traitement de données anonymes.

Infos et recueil des personnes mentionnées : mention types

« Les informations recueillies via le présent appareil par …… *(Veuillez indiquer l'identité du responsable de traitement)* font l'objet d'un traitement informatique destiné à …… *(Veuillez préciser la finalité)*.

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, vous pouvez obtenir communication et, le cas échéant, rectification ou suppression des informations vous concernant, en vous adressant au service …… *(Veuillez citer le nom et les coordonnées du service concerné)*.

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

Si vous acceptez que vos données soient transmises à …… *(Veuillez préciser les catégories de destinataires)* pour …… *(Veuillez préciser la finalité : par exemple, « recevoir des propositions commerciales par voie électronique »)*, merci de cocher la case ci-contre : ☐ *(Cette case ne doit pas être pré-cochée)* ».

Lexique

Personne concernée : la personne concernée est la personne à laquelle se rattachent les données qui sont collectées et traitées. Cette personne pourra également être identifiée dans les fiches pratiques comme l'usager, l'abonné, le client ou le locataire, selon les cas.

Prestataire : le prestataire est celui qui a conclu directement le contrat avec la personne concernée. En tant que responsable de traitement, il doit respecter l'ensemble des obligations imposées par la loi Informatique et Libertés (notamment réalisation des formalités préalables auprès de la CNIL, information ou recueil du consentement de la personne concernée, mise en place de mesures de sécurité adaptées).

Sous-traitant : le sous-traitant est celui à qui le prestataire a confié la réalisation de tout ou partie de la prestation. Il collecte et traite les données uniquement au nom et pour le compte du prestataire. Seule pèse sur lui l'obligation d'assurer la sécurité et la confidentialité des données collectées.

Partenaire commercial : le partenaire commercial est celui à qui le prestataire transmet des données personnelles. Il collecte et traite les données pour son propre compte. Il est donc également responsable de traitement pour les données qui lui sont transmises. Il doit, à ce titre, respecter l'ensemble des obligations imposées par la loi Informatique et Libertés (notamment réalisation des formalités préalables auprès de la CNIL, information ou recueil du consentement de la personne concernée, mise en place de mesures de sécurité adaptées).

Tiers : le tiers est toute personne autre que la personne concernée, qu'il s'agisse d'un prestataire, sous-traitant, ou partenaire commercial.

FIEEC

FEDERATION DES INDUSTRIES ELECTRIQUES, ELECTRONIQUES ET DE COMMUNICATION

www.fieec.fr

CNIL

Commission Nationale de l'Informatique et des Libertés