SCÉNARIO N°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

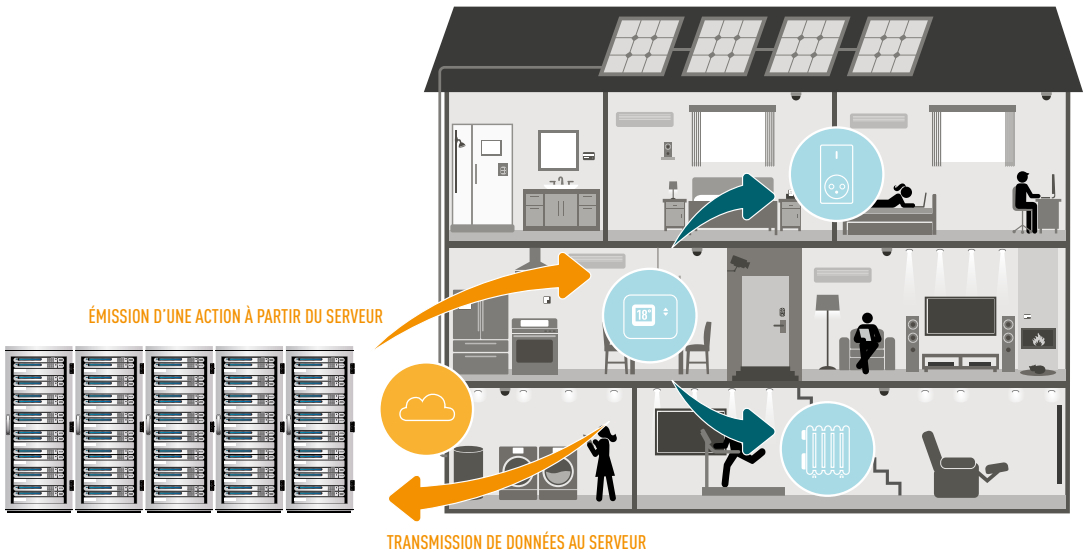
PÉRIMÈTRE

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 un 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).



SCÉNARIO N°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

ANALYSE DES TRAITEMENTS DE DONNÉES PERSONNELLES 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)

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. À 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.

LA GESTION DES DONNÉES COLLECTÉES DANS LE LOGEMENT ET TRANSMISES À L'EXTÉRIEUR POUR PERMETTRE UN PILOTAGE À DISTANCE DE CERTAINS ÉQUIPEMENTS DU LOGEMENT

- 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. À 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.

LA GESTION DES DONNÉES COLLECTÉES DANS LE LOGEMENT ET TRANSMISES À L'EXTÉRIEUR POUR PERMETTRE UN PILOTAGE À DISTANCE DE CERTAINS ÉQUIPEMENTS DU LOGEMENT

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 (http://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). À 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).