CNIL
Commission Nationale de l'Informatique et des Libertés

May 2014 issue

cnil.fr

COMPLIANCE PACKAGE

ON SMART METERS

The compliance package is a new tool for regulating personal data, encompassing the following:

- **A working method:** It allows the CNIL to fully involve the stakeholders of a business sector (professionals primarily, but also, where appropriate, public authorities and concerned users) in order to report on good or bad practices, problems encountered, the demands of users, the specificities of the sector in question and the questions raised in the field.
- **A new regulatory method for the CNIL:** The aim is to build sectoral standards, examining the processing of personal data in the sector from various angles in order to define:
  - a set of rules and best practices, adapted using existing legal means such as simplified standards, single authorisations, recommendations, recognition of compliance with professional rules, but also practical fact sheets developed to clarify and give concrete examples.
  - operating procedures and organisational processes related to the establishment of CNIL recognized personal data protection officers, binding corporate rules (BCR), privacy seals, etc.

This reference framework has a twofold objective:

- **Ensuring the legal security of professionals** by providing practical guidance on how to comply with specific texts and operating procedures.
- **Simplifying formalities** as much as the current law allows by using waivers, simplified standards and single authorisations.

SMART METERS

In recent years, there has been a rapid growth of communicating objects, which are increasingly becoming a part of the everyday life of consumers. The energy sector is particularly affected by the massive influx of communicating products and innovative services.

To function properly, these new products and services may be required to collect and process a very large amount of personal data, such as data on the energy consumption of appliances in the home. The CNIL therefore sought to support industrialists in the sector, as early as the creation stages of these new products and services, by issuing a number of recommendations.

Recommendation on smart meters

Expected to be installed in over 35 million homes by distribution system operators, smart meters call for particular vigilance in order to protect the privacy of data subjects. These devices are capable of collecting the load curve, whose thorough analysis can yield substantial information about the lifestyles of data subjects (i.e., at what time

they wake up and go to bed, periods of absence, number of people in the home, etc.).

Insofar as their installation will be mandatory, the French Data Protection Authority conducted in-depth discussions over the last two years with the stakeholders in order to better regulate the processing carried out by these meters. At the end of these discussions, it adopted a recommendation establishing the framework and the conditions under which people's energy consumption data may be collected and processed.

Deliberation no. 2012-404 of November 15, 2012 on recommendations for processing detailed energy consumption data collected by smart meters.

Innovations in energy management in homes: CNIL-FIEEC partnership

As part of a partnership between the CNIL and the Federation of Electrical, Electronic and Communication Industries (FIEEC), a working group was created to identify the principles that should regulate the collection and processing of energy consumption data by devices installed by users called "downstream electric meters" (for example, directly on the circuit breaker panel, via an outlet on the meter, directly in an electrical outlet).

The Federation of Electrical, Electronic and Communication Industries (FIEEC) represents the interests of trade unions and professional organisations whose members belong to energy, automation, electricity, electronics, digital technology and consumer goods sectors. These sectors include nearly 3,000 companies, employing almost 420,000 people and generate more than €98 billion in turnover, including 46% from exports.

FIEEC's mission is to promote and defend the interests of its members; propose reforms, anticipate and participate in regulatory developments; support companies and clarify the enforcement of technical and legal rules; offer its members privileged contacts with French and European policy makers; and bring together stakeholders in the sectors of its members to provide a single contact person for the Administration.

FINDINGS OF THE WORKING GROUP

The objective of this working group was to produce a publication of best practices intended to boost the innovation of industries in the sector by integrating the protection of personal data as early as possible in the definition of new services, which is called "privacy by design".

This work relates only to the processing of data collected through devices or software installed:

- Outside the meter infrastructure, i.e., downstream electric meters (e.g. directly on the circuit breaker panel or via an outlet on the meter for collecting accurate energy consumption data). As a result, data processing operations carried out directly via electric meters are excluded from the present work;
- Upon the request and under the control of individuals in order to provide them specific services (B to C).

To facilitate the compliance of these devices with the French Data Protection Act, three working assumptions were identified, corresponding to the three scenarios that may be encountered by professionals in the sector. Intended for professionals, these guidelines specify for each type of processing: the intended purposes, the categories of data

collected, the retention period of such data, the rights of data subjects, the security measures to be implemented, and the recipients of the information.

They are designed to be extended to the European level, both by the FIEEC and by the CNIL, to enable stakeholders to position themselves on a European if not global market, making data protection a factor of competitiveness.

The adopted working method is primarily focused on the user, which is a decisive trust factor for consumers so that they opt for these innovative products.

These guidelines are representative of the understanding, at this point in time, of the technologies and associated practices, and they shall be reviewed annually. It is therefore important to underline their flexible and progressive nature.

OVERVIEW

French Data Protection Act

The French Data Protection Act of January 6, 1978 as amended applies to all cases where personal data are processed:

• Processing of personal data means any operation (collection, recording, storage, modification, retrieval, consultation, use, communication, interconnection, destruction, etc.) related to personal data.

• Personal data means any information relating to a natural person identified or who can be identified, directly or indirectly.

Thus, all data, which alone or in combination with others, may be linked to an identified or identifiable user, a customer or a subscriber (temperatures, electricity or gas consumption, amount of hot water used, condition of electrical appliances, etc.) constitute personal data. Personal data are therefore not merely nominal data (besides surname and first name).

Furthermore, even if the data may in practice relate to several people belonging to the same household, the CNIL finds that these are personal data insofar as they are linked to an identified individual (the subscriber).

The processing of personal data shall comply with the French Data Protection Act. Any person wishing to process personal data is subject to a number of legal obligations (informing data subjects about such processing, obtaining their consent, setting-up procedures for the exercise of the right to access and delete data, establishing security measures, completing prior formalities with the CNIL, etc.).

The French Data Protection Act does not apply to processing in the course of purely personal activities (such as the processing described in Sheet 1) or when the processed data are anonymous. In other words, it does not apply when the data cannot be linked directly or indirectly to a natural person by isolating a home.

To determine the mechanism to be implemented for obtaining anonymous data, the service provider shall examine the possibility of re-identifying the individuals from the data obtained. It is therefore necessary to take into account the volume of data, their accuracy, the number of data subjects, etc. Anonymisation mechanisms shall therefore be defined case by case. For example, the aggregation of data for reconstructing the load curves obtained from ten independent homes with the same profile may be considered anonymous. Similarly, an average energy consumption profile built on the basis of the load curves average is also construed as the processing of anonymous data.

SCOPE OF THE 3 PATTERNS OF INNOVATION

Scenario No. 1 "IN → IN": management of data collected in the home without communication to the outside.

In this scenario, the data collected in the home are under the sole control of the user and are not intended to be collected or reused by a third party, which can correspond to two cases:

1. Purely "IN → IN" applications: several products or solutions communicate with each other without transferring data to the outside.

2. Applications which involve a transfer of data from the home without such data being transmitted to third parties for reuse. This is the case of applications for which the data:

- remain confined within communication networks fully under the user's control (such as Wi-Fi or other local networks); or
- circulate in public telecommunication networks (such as ADSL, fibre, GSM).

Scenario No. 2 "IN → OUT": management of data collected in the home and transmitted outside.

In this scenario, the data collected:

- leave the home to be retransmitted to one or more service providers, whether this transfer is materially carried out by the data subject or by the service provider itself;
- are processed by the service provider to offer a service to the data subject, without however triggering an action in the home.

Scenario No. 3 "IN → OUT → IN": management of data collected in the home and transmitted outside to allow the remote control of certain appliances within the home.

In this scenario, the data:

- leave the home to be retransmitted to one or more service providers, whether this transfer is materially carried out by the data subject or by the service provider itself;
- are processed by the service provider to offer a service to the data subject implying an interaction with the home in view of the energy management of the appliances within the home.

GLOSSARY

Data subject: the data subject is the individual to whom the data that are collected and processed are linked. This individual may also be identified in the fact sheets as the user, subscriber, customer or tenant, according to the case.

Service provider: the service provider is the one that has directly entered into contract with the data subject. As data controller, it shall comply with all the obligations under the French Data Protection Act (notably completing prior formalities with the CNIL, informing or obtaining the consent of the data subject, implementing suitable security measures).

Data processor: the data processor is the one to which the service provider has subcontracted the implementation of all or part of the service. It collects and processes data only on behalf of the original service provider. Its only obligation is ensuring the security and confidentiality of the collected data.

- **Business partner:** the business partner is the one to which the service provider transmits personal data. It collects and processes data for its own account. Therefore, it is also a data controller for the data transmitted to it. In this respect, it shall comply with all the obligations under the French Data Protection Act (notably completing prior formalities with the CNIL, informing or obtaining the consent of the data subject, implementing suitable security measures).

- **Third party:** the third party is any person other than the data subject, whether it is a service provider, processor or business partner.

MODEL CLAUSE FOR INFORMING AND OBTAINING THE CONSENT OF DATA SUBJECT

The information collected via this device by _____ *(**Please state the identity of the data controller**) is electronically processed for* _____ *(**Please state the purpose**).*

(Pursuant to Articles 39 et seq. of the amended French Data Protection Act No. 78-17 of January 6, 1978) you may request the disclosure and, where appropriate, the correction or deletion of your personal data, by contacting the department _____ *(**Please mention the name and contact details of the concerned department**).*

You may also, for legitimate reasons, object to the processing of your personal data.

If you agree to your data being transmitted to _____ *(**Specify the categories of recipients**) for* __ *(**Please state the purpose: for example, "receiving sales offers by email"**), please check the box below:*

☐ *(**This box must not be pre-selected**)*

SCENARIO NO. 1 / "IN → IN"
MANAGEMENT OF DATA COLLECTED IN THE HOME WITHOUT COMMUNICATION TO THE OUTSIDE

SCOPE

In this scenario, the data collected in the home are under the sole control of the user and are not intended to be collected or reused by a third party, which can correspond to two cases:

1. Purely "IN → IN" applications: several products or solutions communicate with each other without transferring data to the outside;

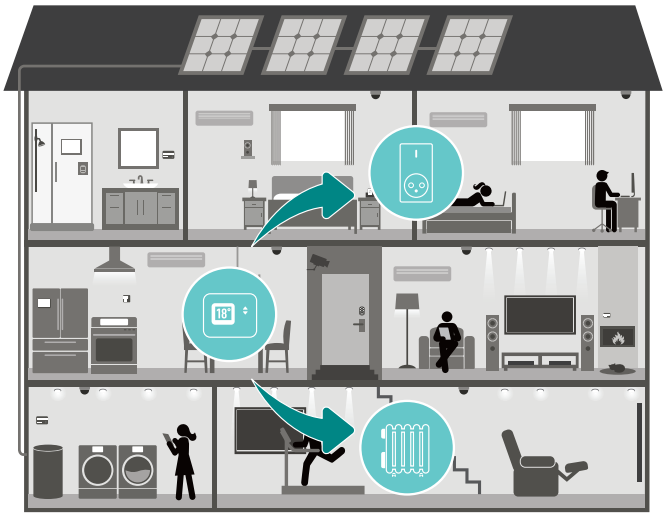
For example: communication between the thermostat and the heating system, managing the heating zone by zone, placing the home in sleep mode when the occupant leaves it, deploying roller shutters based on the level of sunlight or ambient temperature in the zone determined by a sensor.

2. Applications which involve a transfer of data from the home without such data being transmitted to third parties for reuse. This is the case of applications for which the data:

- remain confined within communication networks fully under the user's control (such as Wi-Fi or another local network); or
- circulate in public telecommunication networks (such as ADSL, fibre, GSM).

For example: a smartphone application used by the data subject, which communicates directly with the appliances installed within their home.

The fact that the data are transmitted on networks managed by electronic communications operators does not pose any difficulties insofar as these operators have stringent obligations as to what they can do with such traffic data. This is however only valid if the operator in question acts as the provider of the electronic communication service. Conversely, if the operator wishes to provide another service, the applicable recommendations are those for Scenarios 2 or 3.



SCENARIO NO. 1/ "IN → IN"

MANAGEMENT OF DATA COLLECTED IN THE HOME WITHOUT COMMUNICATION TO THE OUTSIDE

ANALYSIS OF PERSONAL DATA PROCESSING PURSUANT TO THE FRENCH DATA PROTECTION ACT

The processing of personal data must comply with the French Data Protection Act. Any person wishing to process personal data is subject to a number of legal obligations, except for processing performed in the course of purely personal activities, which is the case in the scenario described in this sheet.

Insofar as the devices are under the sole control of the data subject in this scenario, the main issue is that of data security.

Intended purposes of processing:

- **Purpose 1: Managing appliances and energy consumption information:** the data subject wishes to obtain information about their energy consumption or to set up communication between various devices in their home to access home automation or energy efficiency services. For this purpose, they install one or more products (an ecosystem);
- **Purpose 2: energy consumption information in new buildings in accordance with Thermal Regulations 2012 (RT 2012):** the occupant of the home is informed about their energy consumption via devices installed in their home.

Legal basis

The legal basis for the processing is the consent of the data subject:

- For Purpose 1, this consent shall be obtained when the data subject signs the contract with a service provider so that the latter may provide them a specific service. The consent shall therefore be obtained at the time the contract is signed;
- For Purpose 2, occupants of the home shall be capable of controlling the system. They shall therefore be able to deactivate the system themselves or request its deactivation. In fact, RT 2012 requires that the owner/landlord should install a device in the home to inform the occupant about their energy consumption, but the latter may choose not to receive this information.

Consent must be a freely given, specific and informed indication of the data subjects' wishes by which they signify their agreement to the processing of personal data (e.g. checked box that is not pre-selected, connecting a product in the home).

Data collected

Only personal data necessary for the intended purpose of the processing may be collected. In the case of a service contract purchased by the data subject, only data that are essential for the delivery of the service in question may be collected.

Retention period

The retention period for collected data shall be determined by the data subject themselves as they control the system.

Thus, the data subject needs to be able to delete personal data collected by the devices installed in their home, at any time (and notably when the data subject moves out or when a service operation is required, implying that a third party may gain access to the data for updates, repairs, etc.). It should be possible to delete the data through a system provided inside the device (button, disconnection, etc.) or by any other means provided to the data subject.

In any case, when the service provider recovers a device that is not meant to be reinstalled in the data subject's home, it shall systematically delete the data contained in this device. Whereas such deletion of data is essential for refurbished products, it may be done by destroying the device itself for end-of-life products.

Recipients

Insofar as there is no communication to the outside in this scenario, the data subject is the only one with access to the data.

SCENARIO NO. 1/ "IN ➔ IN"

MANAGEMENT OF DATA COLLECTED IN THE HOME WITHOUT COMMUNICATION TO THE OUTSIDE

Information and rights of data subjects

Insofar as the data are processed in the course of purely personal activities, there is no obligation to inform the data subject about such processing.

However, for Purpose 2 (devices installed in the home pursuant to RT 2012), the data subject must be informed of the presence of such devices and the means of deactivating them. Similarly, when such devices collect data other than those specified in the regulation, the data subject must be informed thereof and allowed to deactivate this part of the device.

In addition, the service provider shall carry out an impact study on the possibility for data subjects to:

- obtain a copy of the data in a widely used electronic format, which allows the data to be reused;
- transmit such data to another system in a widely used electronic format.

Security

The service provider must implement measures to guarantee the security and confidentiality of the data processed by the devices that it provides to the data subject, and must take all necessary precautions to prevent any unauthorised person from taking control of such data, notably by:

- encrypting all data exchanges with state-of-the-art algorithms,
- protecting encryption keys from accidental disclosure,
- authenticating devices receiving the data,
- subjecting access to installation control functions to a reliable authentication of the user (password, electronic certificate, etc.)

The measures thus implemented must be adapted to the level of sensitivity of the data and to the control capacities of the devices.

Prior formalities

Insofar as the data are processed in the course of purely personal activities, there are no formalities to be completed with the CNIL.

SCENARIO NO. 2/ "IN → OUT"
MANAGEMENT OF DATA COLLECTED IN THE HOME AND TRANSMITTED OUTSIDE

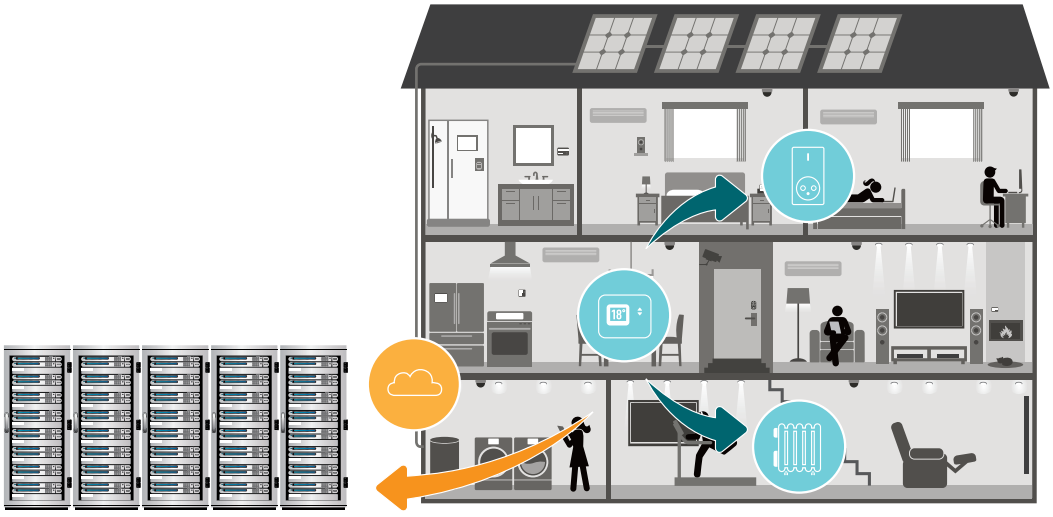
SCOPE

This scenario covers cases in which data:

- leave the home to be then retransmitted to one or more service providers, whether this transfer is materially carried out by the data subject or by the service provider itself;
- are processed by the service provider to offer a service to the data subject, without however triggering an action in the home.

For example: a service provider offers a new electrical contract after analysing the energy consumption.

In practice, the data may be collected and processed by the service provider which has directly entered into contract with the data subject or by third parties to which this service provider has subcontracted the implementation of all or part of the service provision (data processors) or has already transmitted data (business partners).



TRANSMISSION OF DATA TO THE SERVER

SCENARIO NO. 2 / "IN → OUT"

MANAGEMENT OF DATA COLLECTED IN THE HOME AND TRANSMITTED OUTSIDE

ANALYSIS OF PERSONAL DATA PROCESSING PURSUANT TO THE FRENCH DATA PROTECTION ACT

The processing of personal data must comply with the French Data Protection Act. Any person wishing to process personal data is subject to a number of legal obligations.

Intended purposes of the processing (non-exhaustive list)

- **Purpose 1: monitoring of energy consumption in the home:** the data subject enters into contract with a service provider, which provides information about their consumption. In this case, the energy consumption data are transmitted to the service provider to be processed and/or hosted and then made available to the data subject using remote display or a specific platform;
- **Purpose 2: performance of energy audits:** the data subject enters into contract with a service provider, which analyses their energy consumption data and provides them an audit of their consumption to suggest insulation work, new more energy-efficient appliances, etc.
- **Purpose 3: monitoring of energy consumption by social housing landlords:** social housing landlords access energy consumption data to help the tenant reduce their energy consumption;
- **Purpose 4: sales prospection:** the service provider uses the data subject's personal data for sales prospection operations on their behalf;
- **Purpose 5: optimisation of models:** a service provider or social landlord uses the data subject's energy consumption data to compile statistics (anonymised or aggregated data that do not allow a natural person to be identified).

Legal basis

For purposes 1 to 3, the legal basis for the processing is the data subject's consent:

- For Purposes 1 and 2 (the monitoring of energy consumption and the performance of energy audits), this consent must be obtained when the data subject signs the contract with a service provider so that the latter may provide them a specific service. The consent shall therefore be obtained at the time the contract is signed;
- For Purpose 3 (monitoring of energy consumption by social housing landlords), social housing landlords may not ipso facto access the tenant's energy consumption data; they shall therefore obtain the latter's consent. However, they may freely access anonymised data on the building;
- For Purpose 4 (sales prospection), the service provider may freely use data about the data subject (its customer) that are strictly necessary for carrying out sales prospection operations, unless the latter objects to it. However, the CNIL recommends that consent of the data subject should always be obtained before such data are transferred to another service provider.
- For Purpose 5 (optimisation of models), insofar as anonymised data are not personal data, they may be freely used.

Reminder: Consent must be a freely given, specific and informed indication of the data subjects' wishes by which they signify their agreement to the processing of personal data (e.g. checked box that is not pre-selected, connecting a product in the home).

Data collected

Only personal data necessary for the intended purpose of the processing may be collected. In the case of a service contract signed by the data subject, only data that are essential for the delivery of the service in question may be collected.

Retention period

- For Purposes 1 and 2 (requiring the conclusion of a service contract), it is therefore necessary to distinguish the two types of data:
  - **Commercial data (data subject's identity, data about transactions, means of payment, etc.):** such data may be retained for the duration of the contract. At the end of the contract, they may »»

MANAGEMENT OF DATA COLLECTED IN THE HOME AND TRANSMITTED OUTSIDE

be archived physically (on separate media: CD-ROM, etc.) or electronically (for authorisation management) to prevent possible litigation. Thereafter, at the end of the statutory limitation periods, the data shall be deleted or anonymised.

- **Energy consumption data strictly speaking:** such data shall be retained for a period proportionate to the intended purpose:

  - When the contract is for a fixed term ("one shot" service): the energy consumption data may be retained for the entire duration of the contract.
  For example, for Purpose 2 (energy audit), the data may be retained until the results of the analysis are delivered to the data subject.

  - When the contract is concluded for an indefinite period: the data may be retained for a limited period in detailed form, and shall be aggregated for the remainder of the contract period.
  For example, for Purpose 1 (monitoring of energy consumption), it seems reasonable to store detailed data for three years, before aggregation.

At the end of the contract, insofar as the detailed and aggregated energy consumption data are no longer useful for billing purposes, they shall be deleted or anonymised.

- For Purpose 3 (monitoring energy consumption by social housing landlords), the data may be retained for one year in detailed form, and shall be aggregated for the remainder of the lease term.
- For Purpose 4 (sales prospection), the data collected and retained under Purposes 1 and 2, when they are strictly necessary for carrying out sales prospection operations, may be retained by the service provider for a period of three years starting from the end of the business relationship;
- For Purpose 5 (optimisation of models), insofar as anonymised data are not personal data, they may be retained for an unlimited period.

Recipients

In principle, only the data provider and the data subject may access the data.

However, the service provider may be led to transmit the data subject's data to a data processor or to a business partner.

- **Transmission of data to a data processor:** the service provider may freely transmit personal data to a processor, which it calls upon to take part in the implementation of the service offered to the data subject.

In this case, the service provider, as data controller, remains responsible for the conditions under which the data are processed by its processor. For its part, the data processor has the sole obligation of ensuring data security and confidentiality.

- **Transmission of data to a business partner:**
  - If the transmitted data are anonymous data (notably purpose 5): the service provider may freely transmit data to a business partner. Neither the service provider nor the business partner then has any obligation under the French Data Protection Act, which does not apply to anonymous data.
  - If the transmitted data are personal data:

  - For Purposes 1 to 3, the service provider must receive the consent of the data subject before transmitting their data to the business partner (for example, via a check box that is not pre-selected, or where technically possible, via a physical or electronic device in the home accessible to the data subject);
  - For Purpose 4 (sales prospection), the CNIL recommends that consent of the data subject should be obtained systematically.

In both cases, the business partner in turn becomes the data controller for the processing of the data transmitted to it and is subject to all the provisions of the French Data Protection Act.

SCENARIO NO. 2 / "IN → OUT"

MANAGEMENT OF DATA COLLECTED IN THE HOME AND TRANSMITTED OUTSIDE

Information and rights of data subjects

Prior to the processing, the data subject shall be informed of the identity of the data controller, the purpose of the processing, the recipients of the data and the rights they enjoy under the French Data Protection Act. This information may be provided at the time the service contract is signed by the data subject.

Furthermore, the data subject has the right to access, correct and delete their data. The service provider shall enable the data subject to exercise their right of access in the most effective manner possible, knowing that all of the personal data that the service provider holds comes under the purview of this Act.

For Purposes 1 to 3, the data subject may also withdraw their consent by terminating the contract concluded with the service provider, which shall result in the cessation of the processing. The data must then be deleted, anonymised or archived. For Purpose 4 (sales prospection), the data subject shall be able to object, free of charge, to the processing of data by the service provider. For Purpose 5 (optimisation of models), insofar as anonymised data are not personal data, data subjects do not have to be informed.

Further, the service provider shall carry out an impact study on the possibility for data subjects to:

- obtain a copy of the data in a widely used electronic format, which allows the data to be reused;
- transmit such data to another system in a widely used electronic format.

Security

The service provider must implement measures to guarantee the security and confidentiality of the data processed by the devices that it provides to the data subject. It must also take all necessary precautions to prevent any unauthorised person from taking control of such data, notably by:

- encrypting all data exchanges with state-of-the-art algorithms,
- protecting encryption keys from accidental disclosure,
- authenticating devices receiving the data,
- subjecting access to installation control functions to a reliable authentication of the user (password, electronic certificate, etc.)

The measures thus implemented must be adapted to the level of sensitivity of the data.

As regards measures to be implemented in the infrastructure external to the home, the service provider shall conduct a study of the risks posed by the processing in order to identify and implement necessary measures to protect the privacy of the data subjects. The CNIL provides such a method on its website (http://www.cnil.fr/les-themes/ securite /), but other equivalent methods may be used.

Prior formalities

The service provider shall file a normal notification with the CNIL. This notification must be filed on the CNIL's website (www.cnil.fr).

SCENARIO NO. 3 / "IN → OUT → IN"

MANAGEMENT OF DATA COLLECTED IN THE HOME AND TRANSMITTED OUTSIDE TO ALLOW THE REMOTE CONTROL OF CERTAIN APPLIANCES WITHIN THE HOME

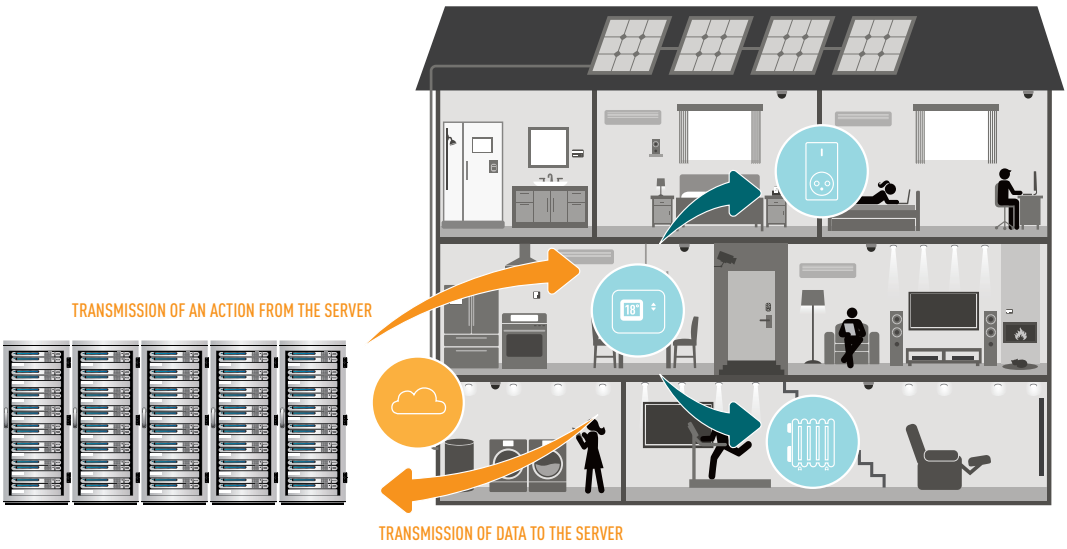
SCOPE

This scenario covers cases in which data:

- leave the home to be then retransmitted to one or more service providers, whether this transfer is materially carried out by the data subject or by the service provider itself;
- are processed by the service provider to offer a service to the data subject implying an interaction with the home in view of the energy management of the appliances in the home.

Example: service allowing the data subject to control the production of domestic hot water, starting their heat pump, starting their washing machine or charging their electric vehicles during periods when electricity is the cheapest.

In practice, the data may be collected and processed by the service provider which has directly entered into contract with the data subject (the service provider) or by other third party service providers to which the original service provider has subcontracted the implementation of all or part of the service provision (data processors).



SCENARIO NO. 3 / "IN ➔ OUT ➔ IN"

MANAGEMENT OF DATA COLLECTED IN THE HOME AND TRANSMITTED OUTSIDE TO ALLOW THE REMOTE CONTROL OF CERTAIN APPLIANCES WITHIN THE HOME

ANALYSIS OF PERSONAL DATA PROCESSING PURSUANT TO THE FRENCH DATA PROTECTION ACT

The performance of personal data processing shall comply with the French Data Protection Act. Any person wishing to process personal data is subject to a number of legal obligations.

Intended purposes of the processing (non-exhaustive list)

- **Purpose 1: demand response in the home:** the data subject enters into contract with a service provider, which provides demand response services, enabling the remote activation or deactivation of certain appliances in the home in certain identified situations and thereby shift their energy consumption. In this case, the data are transmitted to the service provider which processes them to determine when to intervene on the appliances in the home (e.g., service for switching off heating above 19°C during an energy consumption peak);
- **Purpose 2: energy efficiency of the home:** data subject enters into contract with a service provider which provides them a service to improve the energy efficiency of their home by acting on the various appliances in the home. In this case, data are transmitted to the service provider, which processes them to determine the action to be taken in the home (for example, service for closing the shutters when no one is present in the home).
- **Purpose 3: sales prospection:** the service provider uses the data subject's personal data for sales prospection operations on its behalf.

Legal basis

For Purposes 1 and 2 (demand response and energy efficiency), the legal basis for the processing is data subject's consent. This consent shall be obtained when the data subject signs the contract with a service provider so that the latter may provide them a specific service. The consent shall therefore be obtained at the time the contract is signed.

For Purpose 3 (sales prospection), the service provider may freely use data about the data subject (its customer) that are strictly necessary for carrying out sales prospection operations, unless the latter objects to it. However, the CNIL recommends that data subject's consent should always be obtained before such data are transferred to another service provider.

Consent must be a freely given, specific and informed indication of the data subjects' wishes by which they signify their agreement to the processing of personal data (e.g. checked box that is not pre-selected, connecting a product in the home).

Data collected

Only personal data necessary for the intended purpose of the processing may be collected. In the case of a service contract purchased by the data subject, only data that are essential for the delivery of the service in question may be collected.

Retention period

- For Purposes 1 and 2 (requiring the conclusion of a service contract), it is therefore necessary to distinguish the two types of data:
  - Commercial data (data subject's identity, data about transactions, means of payment, etc.): such data may be retained for the duration of the contract. At the end of the contract, they may be archived physically (on separate media: CD-ROM, etc.) or technically (for authorisation management) to prevent possible litigation. Thereafter, at the end of the statutory limitation periods, the data must be deleted or anonymised.
  - Energy consumption data strictly speaking and control data (data about requests for action on appliances in the home and results, if any, of such actions): such data may be retained for a limited period in detailed form, and must be aggregated for the remainder of the contract period. In this particular case, it seems reasonable to retain detailed data for three years, before ag- ➔➔➔

MANAGEMENT OF DATA COLLECTED IN THE HOME AND TRANSMITTED OUTSIDE TO ALLOW THE REMOTE CONTROL OF CERTAIN APPLIANCES WITHIN THE HOME

gregation. At the end of the contract, insofar as the detailed and aggregated energy consumption data are no longer useful for billing purposes, they shall be deleted or anonymised.

- For Purpose 3 (sales prospection), the data collected and retained under Purposes 1 and 2, when they are strictly necessary for carrying out sales prospection operations, may be retained by the service provider for a period of three years starting from the end of the business relationship.

Recipients

In principle, only the data provider and the data subject may access the data.

However, the service provider may be led to transmit the data subject's data to a processor or a business partner.

- **Transmission of data to a data processor:** the service provider may freely transmit personal data to a processor, which it calls upon to take part in the implementation of the service offered to the data subject.

In this case, the service provider, as data controller, remains responsible for the conditions under which the data are processed by its processor. For its part, the data processor has the sole obligation of ensuring data security and confidentiality.

- **Transmission of data to a business partner:**
  - If the transmitted data are anonymous data: the service provider may freely transmit data to a business partner. Neither the service provider nor the business partner then has any obligation under the French Data Protection Act, which does not apply to anonymous data.
  - If the transmitted data are personal data:
    - For Purposes 1 and 2, the service provider must receive the consent of the data subject before transmitting their data to the business partner (for example, via a check box that is not pre-selected, or where technically possible, via a physical or electronic device in the home accessible to the data subject);
    - For Purpose 3 (sales prospection), the CNIL recommends that consent of the data subject should always be obtained.

In both cases, the business partner in turn becomes the data controller for the processing of the data transmitted to it and is subject to all the provisions of the French Data Protection Act.

Information and rights of data subjects

Prior to the processing, the data subject must be informed of the identity of the data controller, the purpose of the processing, the recipients of the data and the rights they enjoy under the French Data Protection Act. This information may be provided at the time the service contract is signed by the data subject.

Furthermore, the data subject has the right to access, correct and delete their data. The service provider must enable the data subject to exercise their right of access in the most effective manner possible, knowing that all of the personal data that the service provider holds comes under the purview of this Act.

For Purposes 1 and 2, the data subject may also withdraw their consent by terminating the contract concluded with the service provider, which shall result in the cessation of the processing. The data shall then be deleted, anonymised or archived. For Purpose 3 (sales prospection), the data subject must be able to object, free of charge, to the processing of data by the service provider.

Furthermore, the service provider must provide a manual disengagement feature in the device allowing the data subject to counter the actions carried out remotely on the appliances in their home (example: restarting the heating that has been cut off as part of an energy consumption management service).

In addition, the service provider must carry out an impact study on the possibility for data subjects to:

- obtain a copy of the data in a widely used electronic format, which allows the data to be reused;

MANAGEMENT OF DATA COLLECTED IN THE HOME AND TRANSMITTED OUTSIDE TO ALLOW THE REMOTE CONTROL OF CERTAIN APPLIANCES WITHIN THE HOME

- transmit such data to another system in a widely used electronic format.

Security

The service provider must implement measures to guarantee the security and confidentiality of the data processed by the devices that it provides to the data subject, and must take all necessary precautions to prevent any unauthorised person from taking control of such data, notably by:

- encrypting all data exchanges with state-of-the-art algorithms,
- protecting encryption keys from accidental disclosure,
- authenticating devices receiving the data,
- subjecting access to installation control functions to a reliable authentication of the user (password, electronic certificate, etc.)

The measures implemented must be adapted to the level of sensitivity of the data and to the control capacities of the devices.

As regards measures to be externally implemented in the infrastructure of the home, the service provider must conduct a study of the risks posed by the processing in order to identify and implement necessary measures to protect the privacy of the data subjects. The CNIL provides such a method on its website (http://www.cnil.fr/les-themes/ securite /), but other equivalent methods may be used.

Finally, the service provider must develop its products and services by incorporating the issue of personal data right from the start (privacy by design). At the very least, the product or service must limit the transfer of data from the home to that which is strictly necessary to deliver the service, and must give priority to decisions made locally over those made outside of the home. The service provider must also promote the anonymisation of data as early as possible in the collection chain. When the data are anonymous, it may be recalled that the French Data Protection Act no longer applies and therefore the data can be retained and exchanged without limitation.

Prior formalities

The service provider shall file a normal notification with the CNIL. This notification must be filed on the CNIL's website (www.cnil.fr).