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

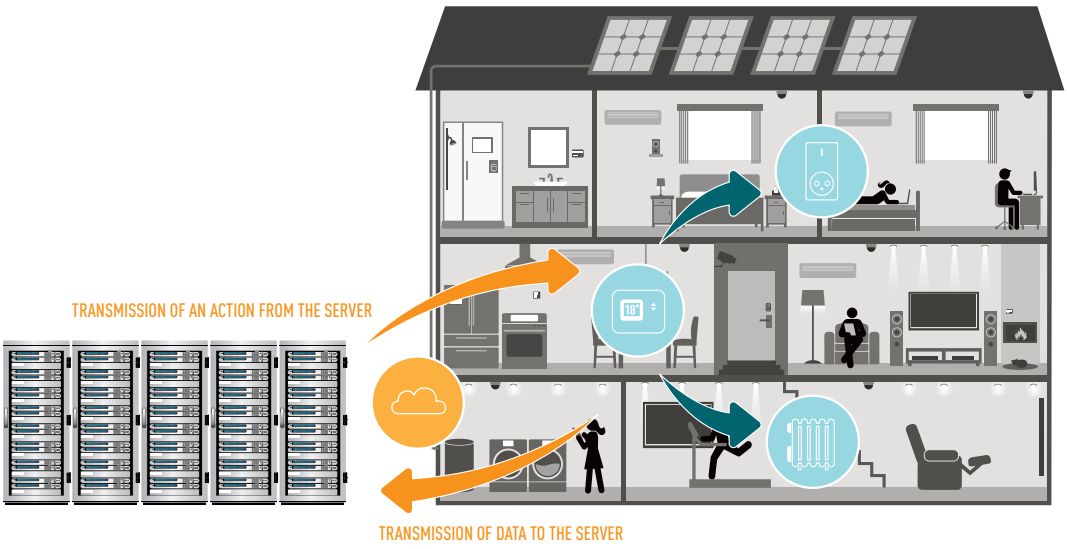
SCOPE

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).