# 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;

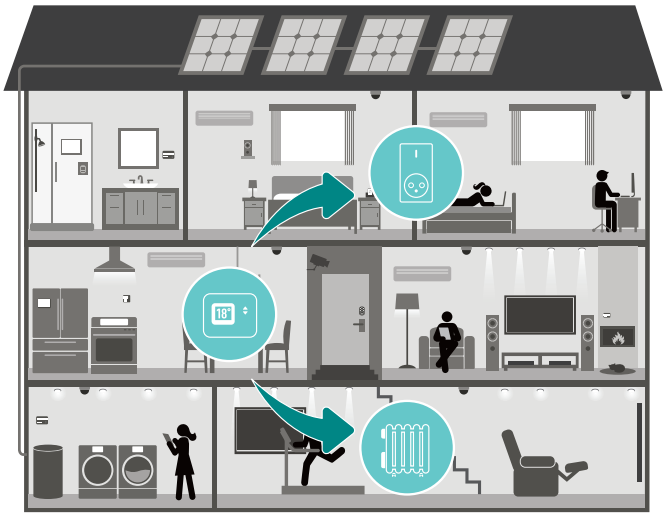
*For example: communication between the thermostat and the heating system, managing the heating zone by zone, placing the home in sleep mode when the occupant leaves it, deploying roller shutters based on the level of sunlight or ambient temperature in the zone determined by a sensor.*

**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.