



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

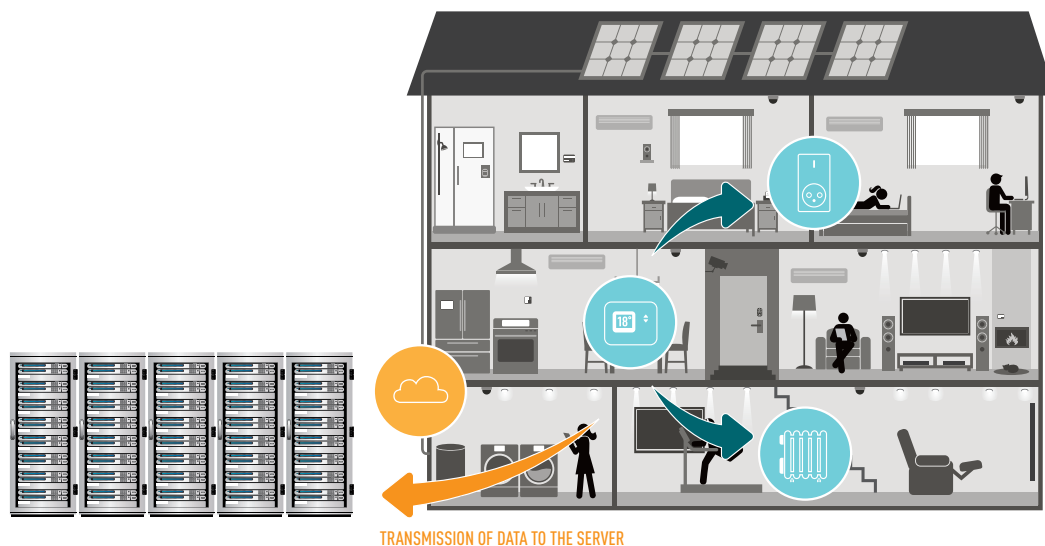
### SCOPE

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).





## 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 prospecting), the data collected and retained under Purposes 1 and 2, when they are strictly necessary for carrying out sales prospecting 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 prospecting), 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.

»»»



## 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](http://www.cnil.fr)).