BoR (17) 13

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

BEREC workshop on **“Enabling the Internet of Things”** Bruxelles, 1 February, 2017

Session 1: Privacy, network security & consumers’ rights

Clémence Scottez, Head of the Economic Sector Department, CNIL (French DPA)

IoT trends

❑ IoT stakeholders aim at offering new applications and services through the collection and the further combination of data about individuals :

- ✓ whether in order to measure the user’s environment ;
- ✓ specific data “only”, or to specifically observe and analyze his/her habits.

WEAR THIS BIOSENSOR SO MANAGEMENT CAN MONITOR YOUR HEALTH DURING THE DAY.
Dilbert.com DilbertCartoonist@gmail.com
WOW. I DIDN'T KNOW YOU CARED SO MUCH ABOUT MY HEALTH.
OH, I DO.
6-15-13 ©2013 Scott Adams, Inc./Dist. by Universal Uclick
EMPLOYEE 479 DOESN'T HAVE SHALLOW BREATHING. YOU CAN GIVE THAT ONE SOME MORE WORK.

Many stakeholders ….
for many uses

❑ Coordinated intervention of device manufacturers :

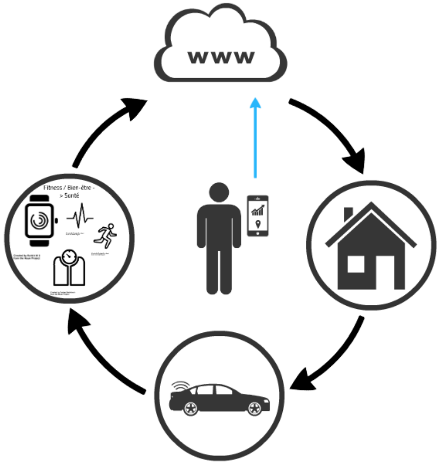
✓ data platforms,

✓ data aggregators or brokers,

✓ application developers,

✓ social platforms, device lenders/renters,

✓ and data subject.



❑ Variety of data and possible interferences.

Privacy risks

- ➢ develop a form of surveillance of individuals ;
- ➢ lack of control and information asymmetry ;
- ➢ incomplete user consent ;
- ➢ multiple purposes of the processing – impossible to foresee different uses ;
- ➢ building behaviour patterns and profiling ;
- ➢ limitation of anonymization ;
- ➢ security risks.

Applicable privacy framework

- ❑ Directive 95/46/EC (Privacy Directive) => futur GDPR
- ❑ Specific provisions of Directive 2002/58/EC as amended by Directive 2009/136/EC (ePrivacy Directive) apply :
  - ➢ to the processing of personal data in connection with the provision of publicly available electronic communication services in public communication networks in the Community ;
  - ➢ to the market player in the IoT value who provides the ECS underlying the IoT service in public communication networks, i.e. the connectivity service provider ;
  - ➢ to the transmission of M2M communications.

New territorial / material scope

- Service providers targeting European people ;
- Whether they are considered as data controller or not ;
- Specific obligations on data processors ;
- Involvement of device manufacturer in the PbD process ;
- New obligations applying to software providers?

New rules to empower users

- **Privacy by Design** principles
- Need for a legal basis :

  => stronger **consent v. legitimate interest**
- Data **portability**
- **Transparency**
- **Accountability**
- **Joint** responsibilities

Which support the WP29 recommendations

- ❑ **General** : perform a DPIA, deletion of raw data, PbDesign and by Default, user friendly features
- ❑ **Device manufacturers** : implement an API and a DNT mode, use of random ID, process the data locally…
- ❑ **Application developers** : respect GDPR rules, allow the data export, not collect any sensitive data
- ❑ **IoT platform** : standards for data export,

aggregated data set, encryption…

In practice ?
The example of smart meters
(french guidelines)

❖**Privacy by design approach to define guidelines for the development of products or services using smart meters data:** increasing the level of customer confidence, limiting privacy risks, giving legal assurance ;

❖ **Working method primarily focused on the user** ;

❖ **Guidelines have a flexible and progressive nature** leaving room for a responsible innovation ;

Compliance package on smart meters - Scope

- **Compliance package on smart meters includes 3 scenarii that may be encountered by professionals from different sectors, using connected devices:**

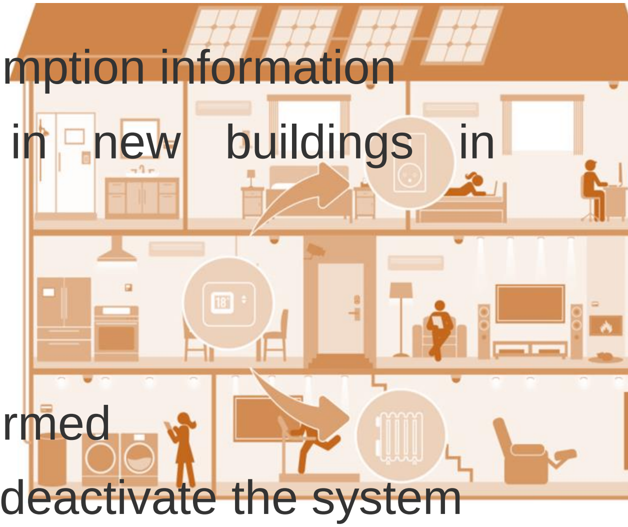
✓Scenario No. 1 ‘IN → IN’: management of data collected in the home without communication to the outside

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

✓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

Scenario No. 1 'IN → IN'

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



INTENDED PURPOSES OF THE PROCESSING

- Purpose 1: Managing appliances and energy consumption information
- Purpose 2: Energy consumption information in new buildings in accordance with Thermal Regulations 2012

LEGAL BASIS

- Purpose 1: Consent – freely given, specific and informed
- Purpose 2: Occupants of the home shall be able to deactivate the system

DATA COLLECTED

- Only personal data necessary for the intended purpose

RECIPIENTS

- Data subject

RETENTION PERIOD

- Retention period determined by the data subject
- Data subject needs to be able to delete personal data at any time
- When the service provider recovers a device, it shall systematically delete the data contained in this device

INFORMATION AND RIGHTS OF DATA SUBJECTS

- Purpose 1: No obligation to inform data subjects about such processing
- Purpose 2: Data subject must be informed of the presence of such devices and the means of deactivating them

SECURITY

Scenario No. 2 ‘IN → OUT’

INTENDED PURPOSES OF THE PROCESSING

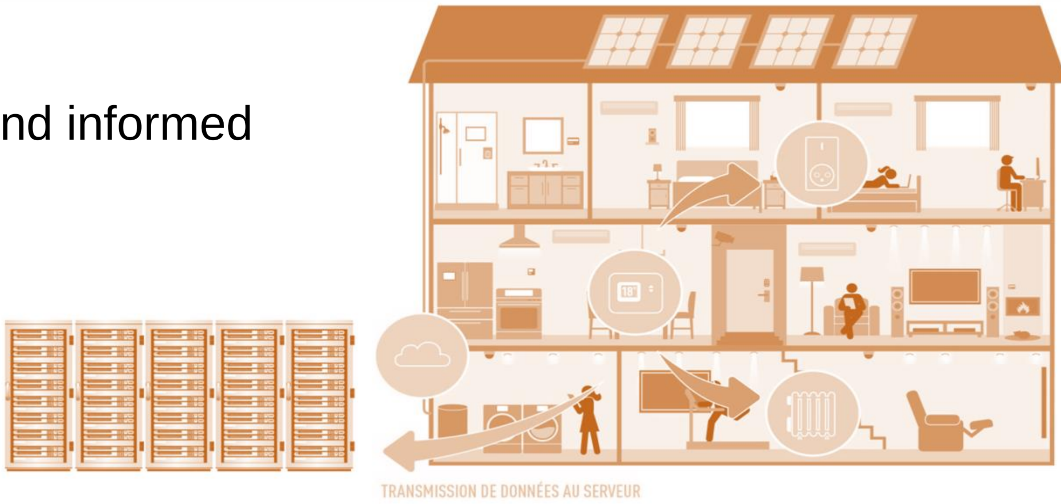
- Purpose 1: Monitoring of energy consumption in the home
- Purpose 2: Performance of energy audits
- Purpose 3: Monitoring of energy consumption by social housing landlords
- Purpose 4: Sales prospection
- Purpose 5: Optimisation of models

LEGAL BASIS

- Consent – freely given, specific and informed

DATA COLLECTED

- Only personal data necessary for the intended purpose
- ……..

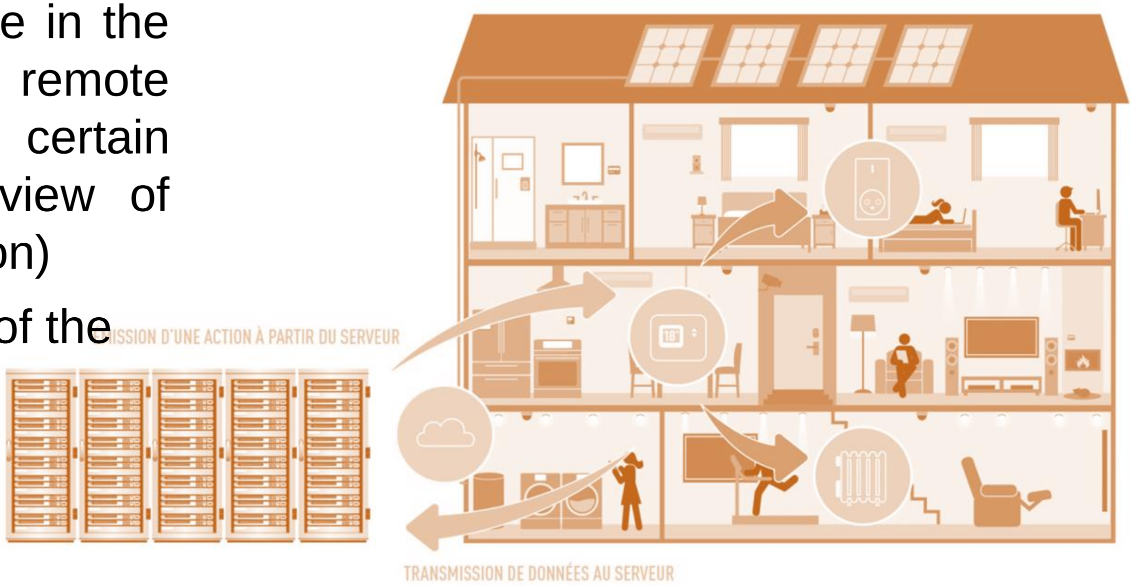


Scenario No. 3 ‘IN→OUT→IN’

Management of data collected in the home and transmitted outside to allow the remote control of certain appliances within the home

■ INTENDED PURPOSES OF THE PROCESSING

- Purpose 1: Demand response in the home (*i.e.*, enabling the remote activation or deactivation of certain appliances in the home in view of shifting their energy consumption)
- Purpose 2: Energy efficiency of the home
- Purpose 3: Sales prospection



ISSION D'UNE ACTION À PARTIR DU SERVEUR
TRANSMISSION DE DONNÉES AU SERVEUR

Thank you for your attention