CNIL

Commission Nationale de l'Informatique et des Libertés

MAIN CHALLENGES IN DATA PRIVACY LAW

AdaptIVe – Legal workshop on “automated driving”

September 17, 2015

Sophie Nerbonne

Head of Compliance – French Data Protection Authority

OVERVIEW ON DATA PROTECTION RULES

- **The data protection European rules (directive 95/46/EC and future regulation to be adopted soon) applies to all cases where personal data are processed**

- **Any person wishing to process personal data is subject to a number of legal obligations**
  - Informing data subjects about such processing (purpose, rights, recipients, transfers…)
  - Setting up procedures for the exercise of the rights (consent, opposition, access, delete data
  - Defining a retention period
  - Establishing security measures
  - In some cases, completing prior formalities with the CNIL in France (notification, opinion or authorization)

- **The Data Protection rules do not apply to processing in the course of purely personal activities or when the processed data are anonymous**

AUTOMATED DRIVING AND DATA PROTECTION: *« how to avoid the crash? »*

- Connected cars have the potential for further progress with regard to environmental friendliness (lower carbon emissions), traffic efficiency, an increase in road safety, etc.

- However, such technical innovations also involve privacy risks that need to be addressed in order to build a customer relationship based on trust

- Indeed, connected cars involve the processing of vast amounts of data that could, if not properly limited and secured, create an architecture of surveillance that could be exploited by governments, corporations and cybercriminals alike

EXAMPLES OF DATA PROTECTION CHALLENGES (1/2)

■ **Example No. 1: Volume and variety of data collected by connected cars *vs* the principles of minimisation, adequacy and transparency**

- Thanks to telematics and wireless connectivity, connected cars will be able to collect very large amounts of data:
  - vehicle-related data: mileage, fuel consumption, vehicle repair and maintenance information, driving habits (speeding, rapid acceleration and braking), but also…
  - driver behavior data, biometrics and health data, location data, personal communications (voice, text, e-mail, social networking), web browsing data, personal contacts and schedules, choice of music, *i.e.*, data highly revealing of personal lifestyles, habits and preferences.

- Such data collecting needs to integrate fundamental data protection principles such as:
  - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
  - Customers shall be informed about categories of processed vehicle data and their purpose
  - Consent / opt-out when necessary: materialized through contractual provisions or technical features (deactivation)
  - Personal data shall not be kept for longer than is necessary
  - Customers have a right to access the data processed about them

EXAMPLES OF DATA PROTECTION CHALLENGES (2/2)

- **Example No. 2: Security risks**
  - Hacking of electronic car systems risks could interfere with control of the vehicle
  - Physical integrity at stake
  - 3 recent examples of data breaches:
    - Ford: Ford's recall of more than 400,000 cars in North America to fix a software bug
    - BMW: Cyber-security flaw affecting the Connected Drive remote-services system
    - Chrysler: the July hacking of a Jeep via its entertainment system

NEW ROLES OF THE DATA PROTECTION REGULATOR

- **Traditional roles:** to protect the rights of citizens (to reinforce digital rights in a digital world), to advise companies (same rules for all companies targeting European market) and public interest

- **Need for the regulator to innovate in implementing a dynamic compliance framework:** the new European regulation (directly applicable) will give stronger enforcement powers to regulators but CNIL believes that sanctions should not be the only mean to regulate data

- **Adaptation within the CNIL structure:** creation of a directorate for compliance (with 4 dedicated "business units", a specific department for DPO's matters and privacy seals and BCR), working with a directorate for innovation and technologies (engineers and futurists updating and forecasting technological evolutions) and a directorate for rights protection (dealing with complaints, controls, injunctions and sanctions).

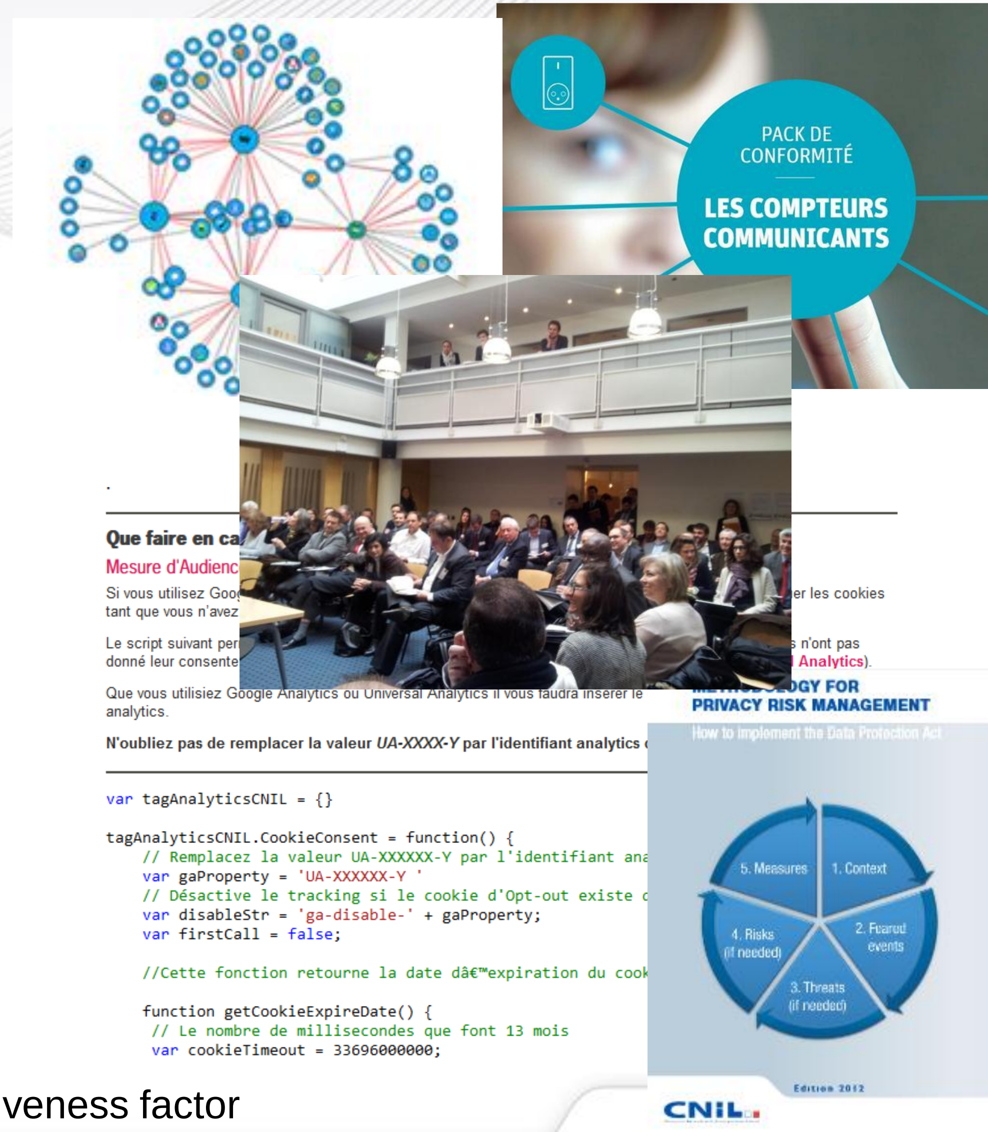
- **Adaptation in the building of compliance tools adapted to** :
  - The exponential pace of technological change
  - The emergence of new business models
  - The development of business ecosystems

CNIL’S COMPLIANCE INSTRUMENTS

- **Examples**
  - Traditional instruments
    - Recommendations
    - Guides and tutorials
  - New instruments
    - Compliance packages and clubs
    - Privacy Seals, BCR
    - Apps, programs, scripts

- **CNIL develops new methods (co-regulation)**
  - multistakholders approach
  - consultation with professionals

- **Different instruments to**
  - meet users’ expectations
  - give guidelines for compliance
  - promote privacy by design as a competitiveness factor



Que faire en ca

Mesure d'Audienc

Si vous utilisez Goo
tant que vous n'avez

er les cookies

Le script suivant per
donné leur consente

s n'ont pas
l Analytics).

Que vous utilisiez Google Analytics ou Universal Analytics il vous faudra insérer le
analytics.

N'oubliez pas de remplacer la valeur *UA-XXXX-Y* par l'identifiant analytics

```
var tagAnalyticsCNIL = {}

tagAnalyticsCNIL.CookieConsent = function() {
    // Remplacez la valeur UA-XXXXXX-Y par l'identifiant ana
    var gaProperty = 'UA-XXXXXX-Y '
    // Désactive le tracking si le cookie d'Opt-out existe d
    var disableStr = 'ga-disable-' + gaProperty;
    var firstCall = false;

    //Cette fonction retourne la date dâ€™expiration du cook

    function getCookieExpireDate() {
     // Le nombre de millisecondes que font 13 mois
     var cookieTimeout = 33696000000;
```

THE COMPLIANCE PACKAGE, A NEW TOOL FOR REGULATING PERSONAL DATA

- **Global approach for one sector:** done with the insurance sector, smart grids and energy management, banking sector, social sector…

- **Elaborated in close cooperation with stakeholders:** true consensus with the stakeholders and active involvement of a key actor, the data protection officer (CIL)

- **Objectives:**
  - Defining and spreading best practices: pragmatic way/case by case approach
  - Ensuring the legal security of professionals
  - Simplifying administrative formalities

- **These guidelines specify for each type of processing:**
  - The intended purpose of the processing
  - The categories of data collected
  - The retention period of such data
  - The rights of data subjects
  - The security measures to be implemented and recipients of the information

THE COMPLIANCE PACKAGE ON SMART METERS – AN ANALYSIS GRID TRANSPOSABLE TO AUTOMATED DRIVING

- **Designed after one year of in-depth discussions with the FIEEC (French professional union of electrical and electronic sector) and represented at the European level by ORGALIME (the European engineering industries association)**

- **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 / not a certification process / need to review periodically

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

Scenario No. 2 ‘IN → OUT’

Management of data collected in the home and transmitted outside

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

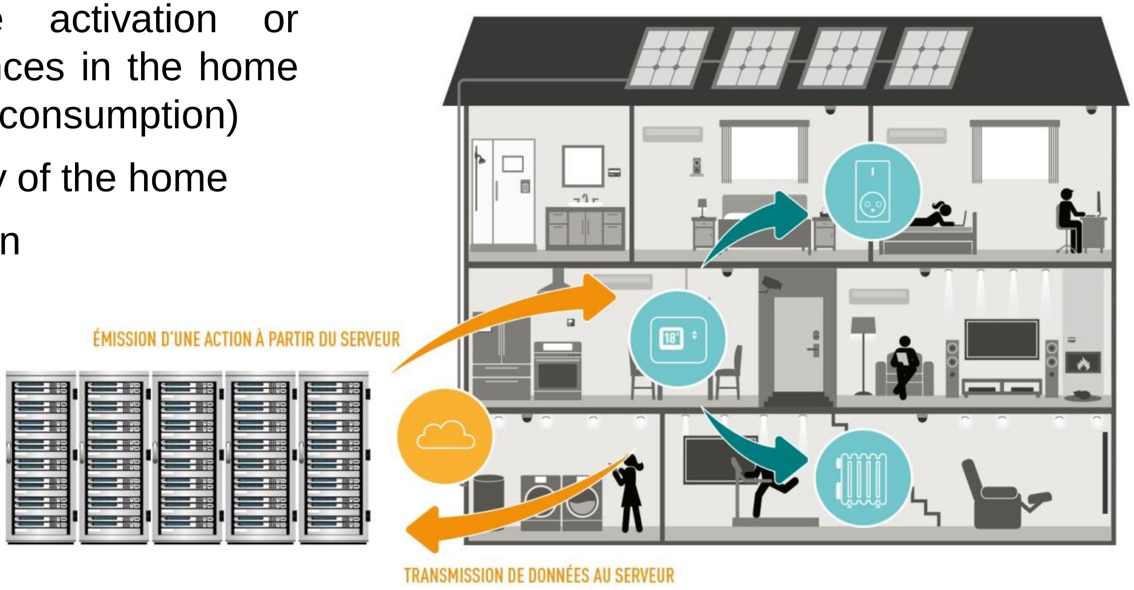
TRANSMISSION DE DONNÉES AU SERVEUR

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

- <u>Purpose 1</u>: 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)
- <u>Purpose 2</u>: Energy efficiency of the home
- <u>Purpose 3</u>: Sales prospection


ÉMISSION D'UNE ACTION À PARTIR DU SERVEUR
18°
TRANSMISSION DE DONNÉES AU SERVEUR

NEXT STEPS

- **The CNIL is currently meeting with the professionals of the automobile sector on privacy issues regarding connected cars to better understand their needs**

- **Aim: to work in 2016 on a compliance package, *i.e.*, flexible and regularly reviewed guidelines, so as to make it simpler for the stakeholders to comply with privacy regulation**

- **Promoting this approach at the European level to enable stakeholders to position themselves on an European if not global market (through the European data protection authorities network, but also the professionals and the European Commission)**

Thank you for your attention

Cf. www.cnil.fr
for more information