Information sessions

The General Data Protection Regulation

Data Protection Impact Assessment (DPIA)

19th October 2017

Esch-sur-Alzette (Belval)

Alain Herrmann

IT department
Agenda

- Goals
- Basic principles and criteria
- Steps of a DPIA
Goals of DPIA

- Setup processings / products/services that respect privacy
- Assess the impacts on private life for the data subjects
- Demonstrate the respect of the GDPR’s fundamental principles
Examples of impacts on individuals

Physical impacts
- Damage to the enjoyment of life, to the aesthetics or economic linked to the physical integrity.

Material impacts
- Suffered loss or missed profit on assets of individuals.

Moral impacts
- Physical or moral suffering, harm to the aesthetic or enjoyment of life

(Source: CNIL)
Examples of physical impacts

- Headaches
- Impairment of bodily integrity, for example, as a result of aggression, domestic accidents, work, etc.
- Defamation that lead to physical or psychical reprisals
- Death (ex: murder, suicide, fatal accident)

(Source: CNIL)
Examples of material impacts

- Loss of time to reiterate steps or wait to realize them
- Targeted online advertising on a privacy aspect that the person wanted to keep confidential (e.g., pregnancy advertising, pharmaceutical treatment)
- Banking ban, property degradation, loss of housing, loss of employment
- Financial peril, large debts, inability to work, inability to relocate

(Source: CNIL)
Examples of moral impacts

- Simple annoyance in regards of the information received or requested
- Minor but objective psychological affection (reputation)
- Victim of blackmail, cyberbullying and moral harassment
- Long-term or permanent psychological disorder, loss of family ties

(Source: CNIL)
What does a DPIA assess?

One processing or a set of similar processing operations

- A « single assessment may address a set of similar processing operations that present similar high risks »
- « there are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a simple project »
**Basic principles**

Data Protection Impact Assessment

Likely to result in high risks? Art 35.(1, 3,4)

- YES
  - Advice of the DPO? Art 39.(1.C)
    - Monitor Performance Art 39(1)(c)
  - Code(s) of conduct Art 35.8
  - Seek the views of the data subjects Art 35.9

- NO
  - Exception? Art 39.(5,10)
    - YES
      - DPIA Art 35.7
    - NO
      - Processing reviewed by the controller Art 35.11

- NO DPIA needed

- Residual high risks? Art 36.1
  - NO
    - No prior consultation Art 35.11
  - YES
    - Prior consultation to the CNPD

Refer to Article 29 guidances
Criterias to perform a DPIA
One processing operation or a set of similar processing operations

- Assessment/profiling
- Automated decision that has a significant legal impact
- Systematic monitoring
- Merges of databases
- Large scale processing
- Sensitive data (Art 9, 10)
- New technologies
- Data on vulnerable persons
- Data transfer outside of the EU
- Any processing operation that makes difficult the exercise of a right

Halle des poches à fonte – 19th October 2017
Examples

<table>
<thead>
<tr>
<th>Processing operations</th>
<th>Possible criterias</th>
<th>DPIA needed ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>An hospital processes genetic and health data of its patients</td>
<td>- Sensitive data</td>
<td>YES</td>
</tr>
<tr>
<td></td>
<td>- Data belonging to vulnerable people</td>
<td></td>
</tr>
<tr>
<td>Usage of a video-monitoring system, to monitor the behaviour of drivers on the highway. Usage of intelligent analysis is planned to read the car numbers</td>
<td>- Surveillance systématique</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Nouvelles technologies</td>
<td></td>
</tr>
<tr>
<td>Internet site using a mailing list to send a newsletter</td>
<td>None</td>
<td>NO</td>
</tr>
<tr>
<td>E-commerce website that displays targeted advertisements based on their visitors consumer habits.</td>
<td>Evaluation / Profiling but not systematic and extensive</td>
<td></td>
</tr>
<tr>
<td>Halle des poches à fonte – 19th october 2017</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
When is a DPIA not needed?

- The risk (for the data subjects) is not high
- A similar DPIA exists: apply the measures
- The law regulates the operation and the DPIA is included in it
- The processing operation is part of the list of DPIA’s exempted processing operations, provided by the CNPD
Iterative process for carrying out a DPIA

1. Description of the envisaged processing
2. Assessment of the necessity and proportionality
3. Measures already envisaged
4. Measures envisaged to address the risks
5. Assessment of the risks to the rights and freedoms
6. Documentation
7. Monitoring and review

Data Protection Impact Assessment

Halle des poches à fonte – 19th October 2017
Data Protection Impact Assessment

**Context**
- Functional description
- Data
- Data carrier
- Etc.

**Risks linked to the security of the data**
- Existing and planned controls
- Risk evaluation

**Fundamental principles**
- Controls to protect the rights
- Proportionnality and necessity

**Validation**
- Assessment (of the previous steps)
- Action plan
- Decision (acceptation of risks)

If needed (DPIA not validated, changes in the processing operation, …)
Publication and consultation

Prior consultation to the CNPD

Needed in case of residual high risk

Transparency: a summary of the DPIA can be made public

The DPIA can be request during a conformity check from the CNPD
The players of a DPIA

The data controller

Data Protection Officer

Chief Information Security Officer

‘Business’ experts

Sectorial experts: legal, ethic, economic

Halle des poches à fonte – 19th October 2017
Define and document roles and responsibilities of the actors involved in a DPIA.
Additional information

DPIA and codes of conduct

Tools to help you

Guidances of the article
29 working group
Data Protection Impact Assessment

Data Protection Governance: exercise of accountability

Certification + code of conducts (Art. 24.3)

Information Security Management System

Security of processings (Art. 32)

Certification + code of conducts (Art. 24.3)

Implementation end to end security

CNPD guide step 4

Data Protection by Design
Data Protection by Default
(Art. 25)

Certification + code of conducts (Art. 24.3)

CNPD Guide step 6

Data Protection Principles
(Art. 5)
- lawfulness, fairness and transparency
- purpose limitation
- data minimisation
- accuracy
- storage limitation
- integrity and confidentiality

CNPD Guide Step 4

Data Subject’s Rights
(Chapter III)

Incident Management

Data Breach
(Art. 33)

to be documented in

Internal data breach record
(Art. 33.5)

Risk for DS

High risk for DS

Notification DPA
(Art. 33)

Communication
Data Subjects
(Art. 34)

CNPD Guide steps 6 + 7

CNPD Guide steps 5 + 7

Re-evaluating risks

Lessons learned

Lessons learned

to implement

CNPD Guide steps 2 + 7

Implement recommendations

Halle des poches à fonte – 19th October 2017