Privacy & Data Protection in IoT and Smart Cities
and something on the ECJ case on Facebook fan pages

Marit Hansen
Data Protection Commissioner
Schleswig-Holstein, Germany

Copenhagen, 28 September 2018

Setting of ULD

- Data Protection Authority (DPA) for both the public and private sector
- Also responsible for freedom of information

Source: en.wikipedia.org/wiki/Schleswig-Holstein
Source: www.maps-for-free.com
Overview

1. Privacy and data protection
2. Risk according to the GDPR
3. Protection goals
4. For IoT, for Smart Cities, for XYZ
5. And a remark on the ECJ case of FB fan pages

Privacy and Data Protection in IoT and Smart Cities

Imbalance in power ⇆ data protection necessary

Important: Perspective of the individual

Privacy and Data Protection in IoT and Smart Cities
Data protection: rights of individuals

Article 1

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

Rights and freedoms of natural persons

EU Charter of Fundamental Rights

• Art. 7 Respect for private and family life (privacy)
• Art. 8 Protection of personal data (data protection)

Processing of data is interference:
• Must be justified
• Interference must be as minimal as possible

• Article 11: Freedom of speech
• Article 12: Freedom of assembly
• Article 21: Non-discrimination
• And others
Overview

1. Privacy and data protection

2. Risk according to the GDPR

3. Protection goals

4. For IoT, for Smart Cities, for XYZ

5. And a remark on the ECJ case of FB fan pages

Not just any risk

Recital 75 of the GDPR

(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage, where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements; in order to create or use personal profiles, where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.
GDPR risk framework

- Risk sources
  - processor/controller
  - third parties (IT security)
  - adverse events (safety)

Risk = severity of potential damage × likelihood

- But cannot be quantified
- Can be approximated objectively

Risk for rights must be mitigated with technical and organisational measures, etc. to protect rights

→ Arts 24, 25, 32, 35 GDPR

Privacy and Data Protection in IoT and Smart Cities
Overview

1. Privacy and data protection
2. Risk according to the GDPR
3. Protection goals
4. For IoT, for Smart Cities, for XYZ
5. And a remark on the ECJ case of FB fan pages

Protection goals: more than IT security

- Confidentiality
- Unlinkability
- Integrity
- Intervenability
- Transparency
- Availability

*) From the data subject’s perspective

classical IT security protection goals*)
Overview

1. Privacy and data protection

2. Risk according to the GDPR

3. Protection goals

4. For IoT, for Smart Cities, for XYZ

5. And a remark on the ECJ case of FB fan pages
**IoT + Big Data (+ AI)**

- Everything can communicate with everything
- Everything produces data trails
- Naïve implementation: everything is linkable

- Range of key questions:
  - Personal data or non-personal data?
  - Accumulation of non-personal data still non-personal data?
  - Risks? (more than indiv. privacy)
  - Who is in control?

---

**Privacy and Data Protection in IoT and Smart Cities**

- Art. 25 GDPR: Data Protection by Design and by Default
- Anonymisation, pseudonymisation (e.g. attribute-based credentials), early erasure, encryption, access control ...

---

**Smart Cities - personal data?**

- Connected Cars Can Build A Better Map
- Use your connected vehicles to maintain, improve and augment the navigation map and content layers

**Smart Cities - personal data?**

Understanding Your Drivers

A full solution that lets OEMs collect, manage, explore and interpret driver analytics
Improve design efficiency, launch innovative marketing and CRM initiatives and more

http://cloudmade.com/solutions/car-driver-analytics

---

**Smart Home: Who is in control?**

Best starting point:
Unlinkability

Image: geralt via Pixabay

Photo: ivanacoi via Pixabay
Smart Cities: Who is in control?

Best starting point: Unlinkability

Privacy and Data Protection in IoT and Smart Cities

Future: ubiquitous sensors

“Asking the user” wouldn’t work; consequences when deactivating sensors?
Overview

1. Privacy and data protection
2. Risk according to the GDPR
3. Protection goals
4. For IoT, for Smart Cities, for XYZ
5. And a remark on the ECJ case of FB fan pages

ECJ case on Facebook fan pages

Question:
Is a company (co-)responsible for Facebook's data processing when administrating a fan page?
☐ No, never?
☐ In a controller-processor relationship?
☐ Joint controllership?

Original Schleswig-Holstein case in 2011
**ECJ ruling:**

**Joint controllership**

- Broad definition of the controller to protect individuals: alone or jointly with others determines purposes and means of the processing
- Primarily Facebook controller (No. 30)

- And the fan page administrator?
- Processing enables advertising business model
- Processing enables fan page administrator to obtain statistics:
  - Definition of parameter for producing statistics (No. 36)
  - In particular demographic data (No. 37)
  - Opportunity to place cookies (No. 35)

 ⇒ Fan page administrator takes part in determination of purposes and means (Rn. 39)

**ECJ case on Facebook fan pages**

**Question:**
Is a company (co-)responsible for Facebook's data processing when administrating a fan page?
- No, never
- In a controller-processor relationship
- Joint controllership! (Art. 26 GDPR)

Note: own purposes of FB Transposition to other providers?!
Conclusion

• Data protection by design and by default
  ▪ Demanded by the GDPR
  ▪ Thereby to be demanded by controllers
  ▪ Rights and freedoms

• GDPR as game changer?
  ▪ Promise of a level playing field
  ▪ Innovation with data protection should conquer ignorant or even privacy-invasive services
  ▪ Good solutions have to be made visible!

Source: congerdesign via Pixabay