

The Future of IoT: Toward More Secure and Human-Centered Devices

Marit Hansen
Data Protection Commissioner
Schleswig-Holstein, Germany



Berlin, 27 November 2019



www.datenschutzzentrum.de

Schleswig-Holstein	
State of Germany	
	
	
Coordinates: 54°28'12"N 9°30'50"E	
Country	Germany
Capital	Kiel
Government	
• Body	Landtag of Schleswig-Holstein
• Minister-President	Daniel Günther (CDU)
• Governing parties	CDU / Greens / FDP
• Bundesrat votes	4 (of 69)
Area	
• Total	15,763.18 km ² (6,086.20 sq mi)
Population (2016-12-31) ^[1]	
• Total	2,881,926
• Density	180/km ² (470/sq mi)

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

The Future of IoT: Privacy



Source: www.maps-for-free.com

Overview



 Photo: Ashtyn Renee
 Unter CC BY 2.0-Lizenz
<https://creativecommons.org/licenses/by/2.0/>

1. Privacy and data protection
2. Risk according to the GDPR
3. Protection goals
4. Reality check:
current IoT
implementation?
5. Demands for future IoT

Imbalance
in power
⇒
data protection
necessary

Important:
Perspective of
the individual



 Photo: beludise via Pixabay

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.

General Data Protection
Regulation (EU) 2016/679

The Future of IoT: Privacy and Data Protection

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

The Future of IoT: Privacy and Data Protection

Overview



 Photo: Ashtyn Renee
 Unter CC BY 2.0-Lizenz
<https://creativecommons.org/licenses/by/2.0/>

1. Privacy and data protection

2. Risk according to the GDPR

General Data Protection
 Regulation (EU) 2016/679

3. Protection goals

4. Reality check:
 current IoT
 implementation?

5. Demands for future IoT

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, religion 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)



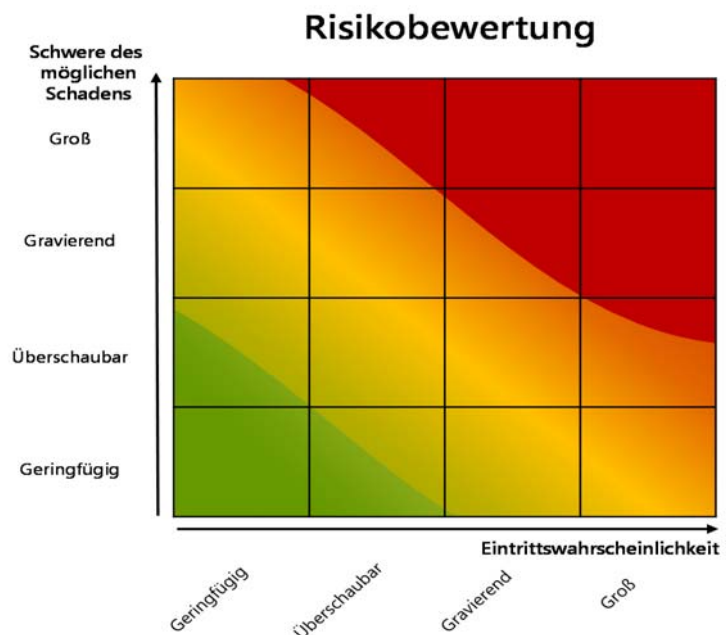
 Photo: beludise via Pixabay



The Future of IoT: Privacy and Data Protection

GDPR risk framework

- Risk = severity of potential damage x 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



The Future of IoT: Privacy and Data Protection

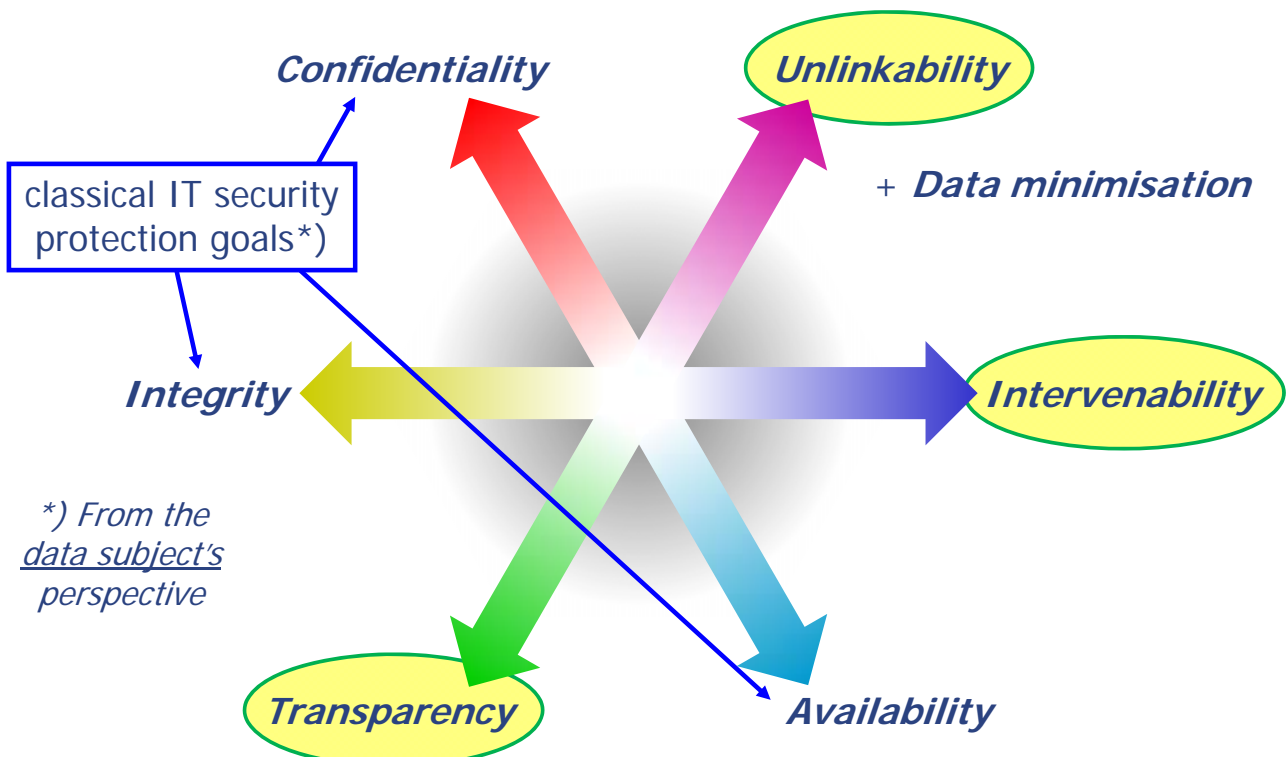
Overview



Photo: Ashtyn Renee
 Unter CC BY 2.0-Lizenz
<https://creativecommons.org/licenses/by/2.0/>

1. Privacy and data protection
2. Risk according to the GDPR
3. **Protection goals**
4. Reality check:
current IoT
implementation?
5. Demands for future IoT

Protection goals: more than IT security



Unlinkability



Separation of domains, separation of power, purpose binding

Photo: ivanacoi via Pixabay

Please, help me!

E.g. opt-out, complaints, judicial relief, reversing decisions ...
deactivating sensors and data processing, defined help desk ...



Photo: geralt via Pixabay

Intervenability

The Future of IoT: Privacy and Data Protection

How to implement?

Transparency



Objective: awareness, understanding and control; different media, support by technology

Photo: geralt via Pixabay

Objective: **risk mitigation** –
i.e. of the risk for the rights and freedoms of natural persons

Overview



Photo: Ashtyn Renee
Unter CC BY 2.0-Lizenz
<https://creativecommons.org/licenses/by/2.0/>

1. Privacy and data protection
2. Risk according to the GDPR
3. Protection goals
4. **Reality check: current IoT implementation?**
5. Demands for future IoT

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?**



Image: jeferrb via Pixabay

Art. 25 GDPR:
Data Protection by Design
and by Default

Anonymisation,
pseudonymisation
(e.g. attribute-based
credentials), early
erasure, encryption,
access control ...

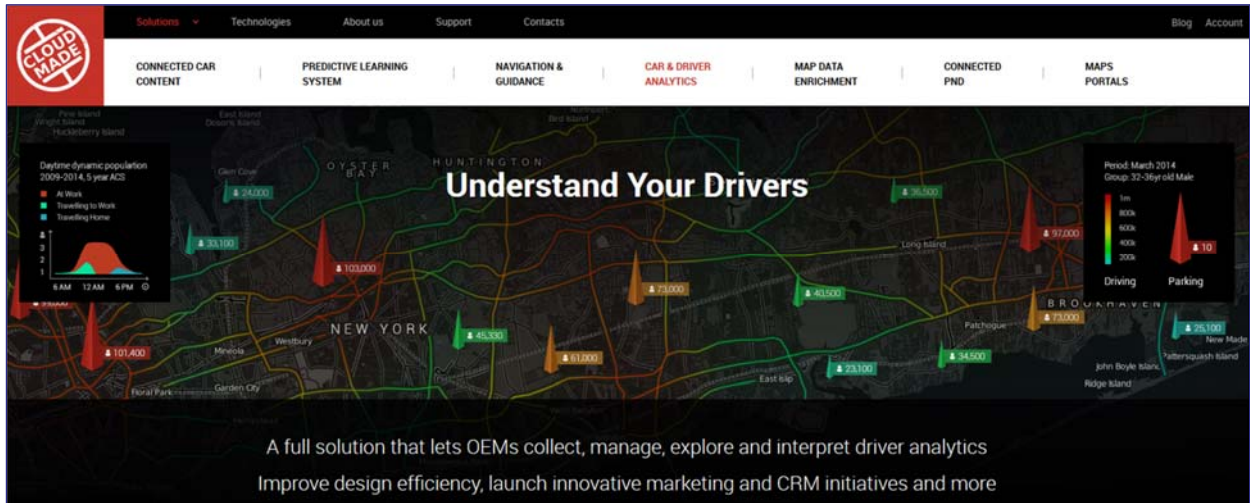
Smart Cities – personal data?

Connected Cars Can Build A Better Map

Use your connected vehicles to maintain, improve and augment the navigation map and content layers

<http://cloudmade.com/solutions/map-data-enrichment>

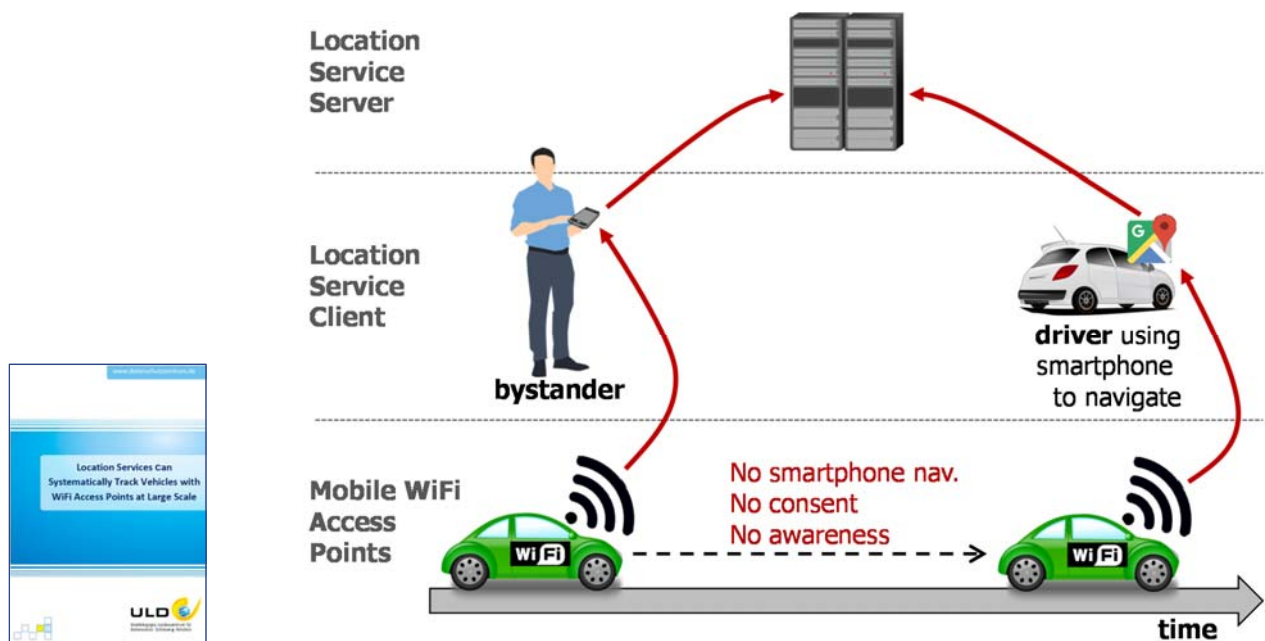
Smart Cities – personal data?



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

The Future of IoT: Privacy and Data Protection

Connected cars as WiFi Access Points, can be tracked



https://www.datenschutzzentrum.de/uploads/projekte/ULD_Location-Service-Tracking.pdf (2019)

The Future of IoT: Privacy and Data Protection

Smart Home: Who is in control?



 Image: geralt via Pixabay

Best starting point:
Unlinkability



 Photo: ivanacoi via Pixabay


Smart Cities: Who is in control?

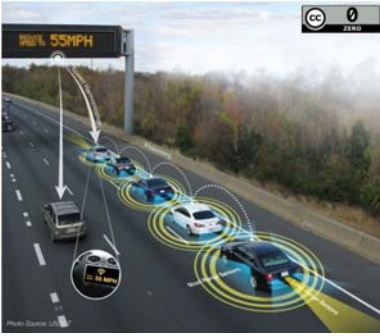


 Photo: geralt via Pixabay

Best starting point:
Unlinkability



 Photo: ivanacoi via Pixabay



IoT: ubiquitous sensors

"Asking the user" wouldn't work;
consequences when deactivating sensors?



Image: 5g.co.uk



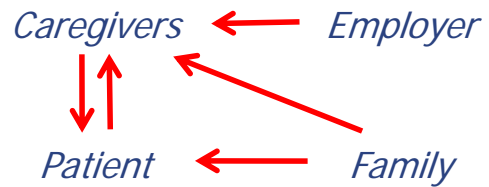
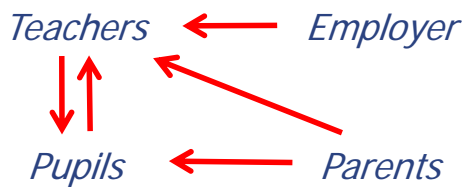
Not to forget: Tech Abuse in Smart Environments



Image: Free-Photos via Pixabay



Image: WikiImages via Pixabay



Not to forget: Tech Abuse in Smart Environments



Tech Abuse – Smart, Internet-connected devices present new risks for victims of domestic violence & abuse


- 1 Wearable devices**
Could allow perpetrators to track and monitor movements and other behavioural patterns drawing on GPS signals and other collected data.
- 2 Phones**
Could provide perpetrator an access point to control various IoT devices.
- 3 Laptops and tablets**
Accounts between devices are linked and could allow perpetrators to change and review IoT devices' settings via an Internet browser.
- 4 Remote control of heating, lighting and blinds**
Could be used to coerce and intimidate victims by switching systems on or off from afar.
- 5 Security cameras and TVs**
Could facilitate remote monitoring and online stalking; video recording could facilitate image-based abuse (such as revenge porn).
- 6 Smart security**
Could provide access to doors through voice activation, apps, or electronic key codes.
- 7 Audio recording**
Could facilitate remote monitoring and stalking.
- 8 Voice control**
May enable perpetrators to contact the victim as well as trace and review a person's history of commands and purchases.
- 9 Router**
Connects all smart home devices to the Internet.

<https://pbs.twimg.com/media/Ds7fJIPWsAA5t7G?format=jpg&name=large> (2019)
Leonie Tanczer, UCL, London - <http://www.csap.cam.ac.uk/network/leonie-tanczer/>

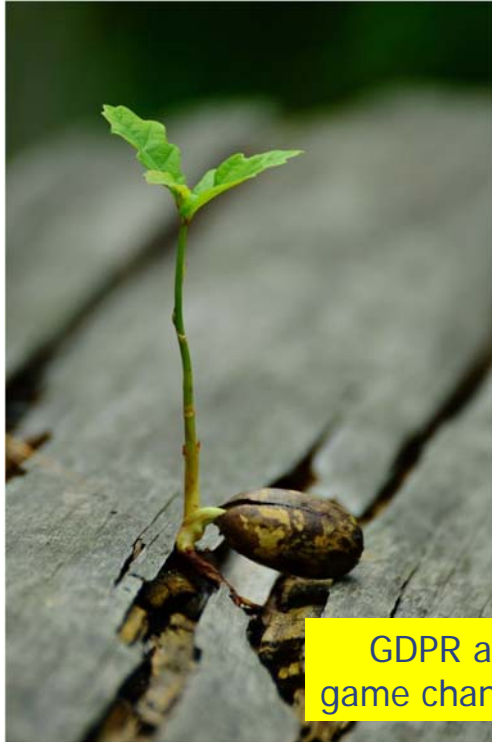
Overview



1. Privacy and data protection
2. Risk according to the GDPR
3. Protection goals
4. Reality check:
current IoT
implementation?
5. **Demands for future IoT**

 Photo: Ashtyn Renee
Unter CC BY 2.0-Lizenz
<https://creativecommons.org/licenses/by/2.0/>

Demands for future IoT



GDPR as
game changer?

- Data protection by design and by default
 - Demanded by the GDPR
 - Thereby **to be demanded by controllers**
- **Liability** of manufacturers?
- Current IoT
 - Not only teething trouble!
 - Obviously **insufficient incentives** to do it right
 - Innovation with data protection should **conquer** ignorant or even privacy-invasive services

 Source: congerdesign via Pixabay