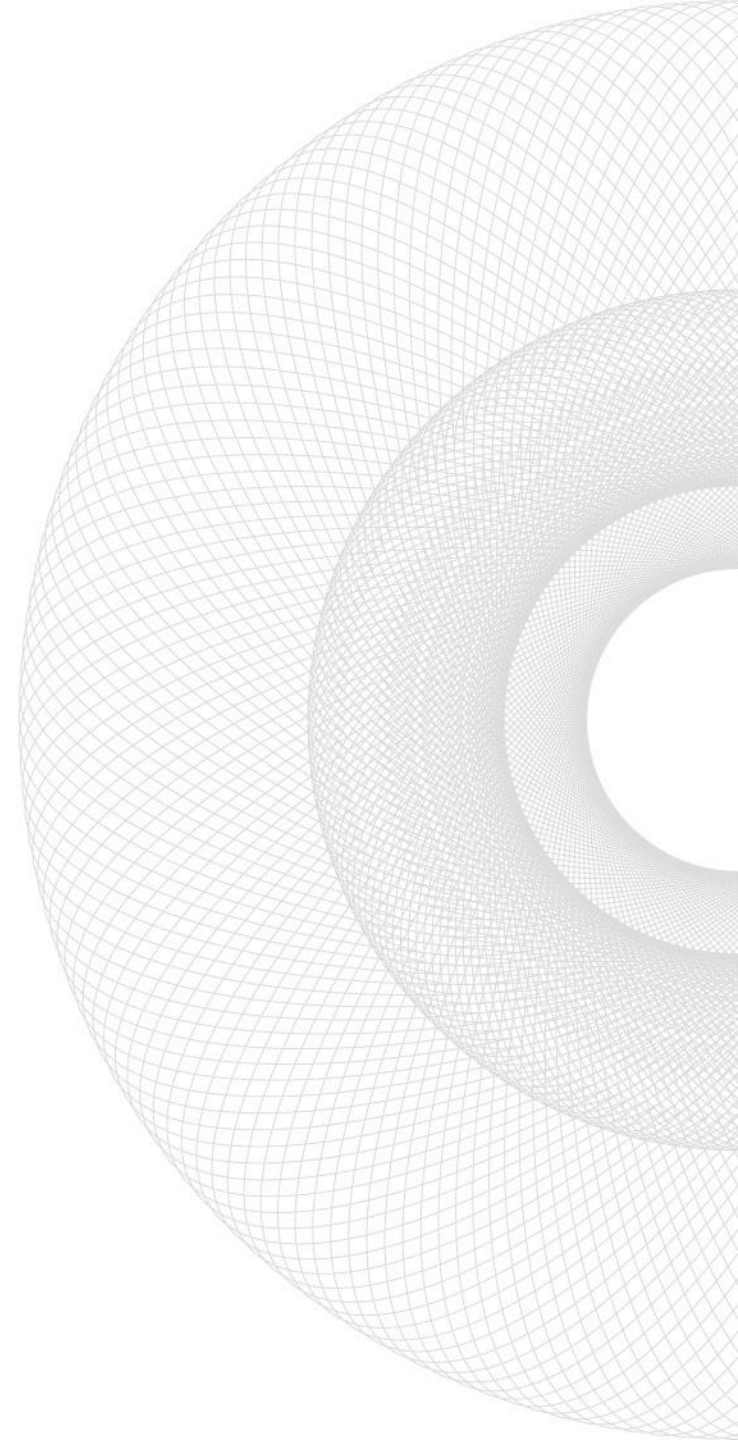


Overview legal concerns IoT

Larisa Găbudeanu, Kinstellar

KINSTELLAR



Content

- I. Overview legal implications
- II. Data privacy aspects
- III. Household case study
- IV. Smart cars case study



I. Overview legal implications

Level 1 – Platform infrastructure and software

- Malfunctioning, interoperability

Level 2 – IP rights

- Ownership of databases and other IP rights
- Licensing matters

Level 3 – Contracting for data

- Commercial agreements, outsourcing structures and level of liabilities
- Ownership of data
- Liability issues depending on structure of data transfers
- Trade secrets (specific legislation)
- Different points of view: all stakeholders, machine producers, service providers, maintenance services
- Competition law matters
- Employment law

Level 4 – Data regulation

- Transparency, accountability and minimization principles
- Specific issues for certain sectors – energy, financial services
- Data transfers; use of sub-contractors;
- Cross-border approach
- Consumer protection

Level 5 – Information management and security

- Sensitive data – e.g. hospitals, eHealth supply chain
- Cybersecurity legislation
- National security/critical infrastructures
- Criminal law implications
- Strategy
- Policies and procedures/processes

II. Data privacy aspects

- **Risk considerations**

- Pseudo-anonymization; identifiers
- Processing and transfer of data to third parties

- **Risk Mitigation Goals and Areas**

- Accountability and transparency principles
- Data minimization principle (e.g. use of health data or from which health data can be inferred)

- **Expectations**

- Establishing risk-based approach in terms of input/processing/out of data

- **Challenges**

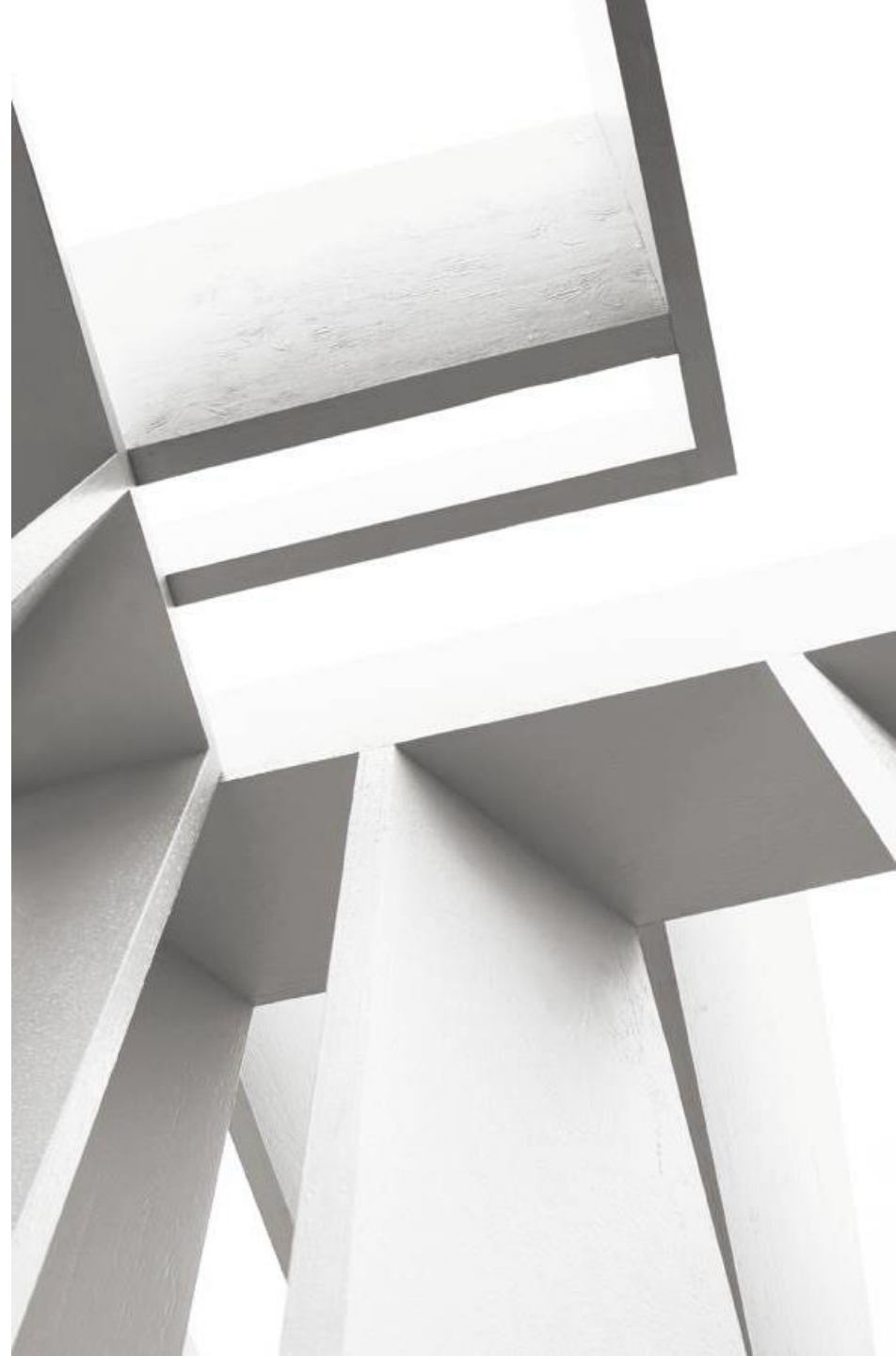
- Profiling and automated decision making
- Secondary uses of data

Approach taken by **regulatory entities and private associations**

- EC: Consultation paper, Working document on liability for emerging digital technologies
- NIST and SANS – whitepapers
- ENISA – security recommendations for IoT; cybersecurity and resilience of smart cars

III. Household case study

- Types of **data devices**: speaker assistance, smart security, thermostats, light devices, switches, smart appliances
- Specific aspects for discussion:
 - Pseudo-anonymization
 - Location of data stored
 - Accuracy and minimization of data
 - Automated decisions
 - Secondary uses of data (e.g. marketing, insurance)



IV. Smart cars case study

- **Types of data:** long terms patterns generated by sensors
- Specific aspects for discussion:
 - Special types of data (e.g. biometrics, health data)
 - Data minimization principle
 - Secondary uses of data (e.g. marketing, insurance)
 - Exercise of data subject rights





Questions?

Thank you!