# AI Act High-Risk Requirements Readiness: Industrial Perspectives and Case Company Insights

**Matthias Wagner**, Rushali Gupta, Markus Borg, Emelie Engström, Michal Lysek

Dept. of Computer Science

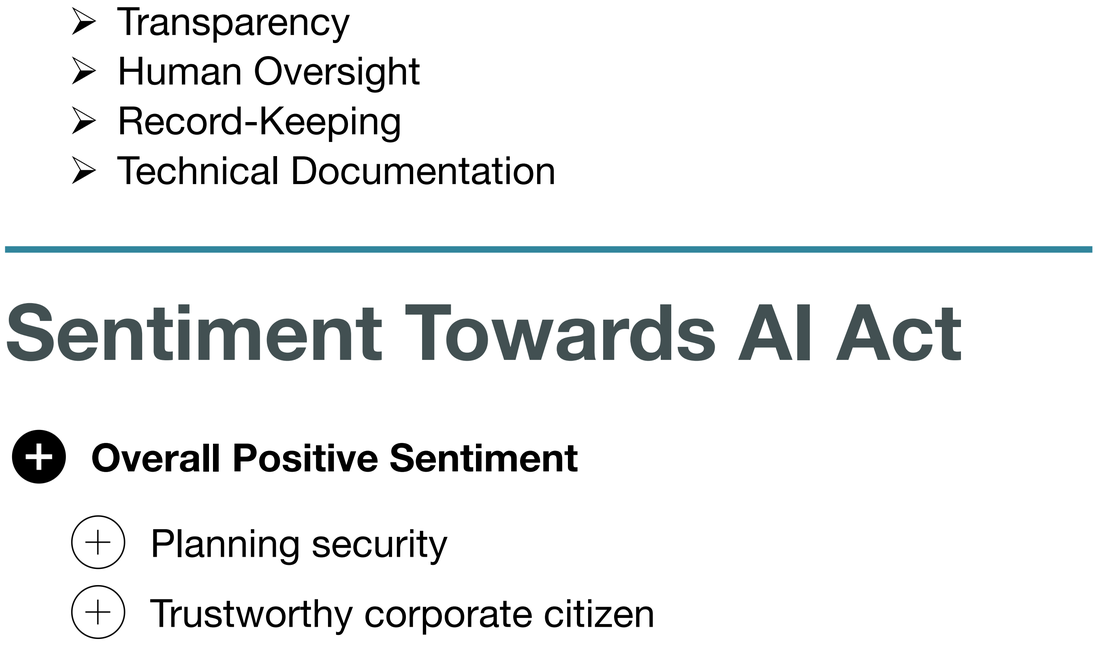
## Problem & Objective

- **AI Act compliance** – Where to start and what to focus on?
- Identify AI Act **high-risk aspects challenging** to **industry**
- Focus **future research** on **pressing** & **relevant aspects** for AI Act **operationalization**

## Case Company

- **Security** & **surveillance** industry
- Leading in **network video solutions**
- **Active** AI Act **engagement** mostly within **legal department** (at time of interviews)

## AI Act Risk-based Approach




**High-Risk Requirements:**

- Risk and Quality Management System
- Data Quality and Governance
- Accuracy, Robustness, and Cybersecurity
- Transparency
- Human Oversight
- Record-Keeping
- Technical Documentation

## Sentiment Towards AI Act

**Overall Positive Sentiment**

- Planning security
- Trustworthy corporate citizen

**Negative Aspects**

- Very broad & extent of coverage uncertain
- High workload expected

## Semi-Structured Interviews

**Case Company**
6 Interviewees

**Broader Industry Perspective**
3 Independent Experts

- 9 Interviews
- ~ 55 min/ Interview
- Middle/Upper Management
- ☑ Pilot Interview
- ☑ Anonymization
- ☑ Multi-Researcher Cross-Validation

## Case Company Readiness

**Well-Established Practices**

- High cybersecurity maturity
- Human oversight
- Record-keeping
- Technical documentation

**Open Challenges**

- Data quality and governance
- Accuracy & robustness
- Customer-oriented performance testing
- Post-market monitoring (Art 72)
- Right to explanation of individual decision-making (Art 86)

WASP WALLENBERG AI, AUTONOMOUS SYSTEMS AND SOFTWARE PROGRAM