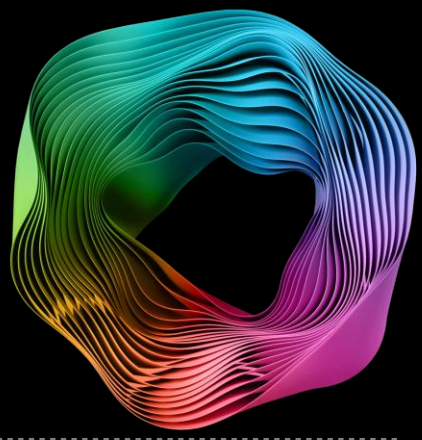
Deloitte.
Legal



Cybersecurity & Law

The Age of Digital Threats

Cyberattacks, data breaches, and critical infrastructure failures rank among the most serious business risks of our time. With EU cyber regulations and growing national regulations, a complex, rapidly changing regulatory environment is emerging. Companies are forced to align technical security measures with legal compliance requirements—and they must do so at a time when the threat landscape is becoming increasingly complex and growing exponentially. Those who fail to act proactively risk hefty fines, liability claims, and reputational damage.

Legal Framework and Areas of Action

Cybersecurity regulation is complex and encompasses both European and national law. Key regulatory frameworks include the **NIS2 Directive** (Network and Information Security), the **EU Cyber Resilience Act (CRA)**, the **DORA Regulation** (Digital Operational Resilience for the Financial Sector), the **IT Security Act 2.0**, the **GDPR**, and industry-specific requirements from the energy, healthcare, and financial sectors.

This gives rise to the following key areas of action in particular:

- **Cyber Compliance** – Implementation of statutory cybersecurity obligations
- **Incident Response** – Legally compliant response to security incidents
- **Supply Chain Security** – Contract Drafting and Liability Issues
- **KRITIS Regulation** – Operator obligations for critical infrastructure
- **Data Protection & Cybersecurity** – Identification of Interfaces and Areas of Conflict

Legal, Operational, and Strategic Challenges

The legal management of cybersecurity risks operates within a field of tension: **regulatory compliance** versus **operational flexibility**, **reporting obligations** versus **strategic communication**, **dependence on third-party providers** versus **self-directed compliance**. Added to this are liability issues in the event of security incidents, requirements for logging and record-keeping, and the legally compliant integration of cloud services and AI-powered security systems. The cross-border nature of cyber threats, in particular, makes a holistic, interdisciplinary approach essential.

Why Act Now? **Investing early in a legally compliant cybersecurity strategy reduces liability risks, avoids fines, and protects your reputation as a reliable and trustworthy market participant - in the eyes of customers, partners, and authorities alike.**

AREAS OF ACTION

Companies that operate IT infrastructures, develop digital products, or provide critical services face the challenge of reconciling technical security requirements with an increasingly stringent regulatory framework. It is crucial to address cybersecurity obligations from an early stage and identify relevant measures.

Tasks

- ✓ **NIS2 Readiness Assessment** – Analysis of Impact, Evaluation of Reporting Requirements, and Implementation Planning in Accordance with the NIS2 Directive and National Implementing Legislation
- ✓ **Cyber Resilience Act (CRA) Compliance** – Ensuring product requirements for manufacturers of networked devices and software throughout the entire lifecycle
- ✓ **DORA Compliance** – Meeting operational resilience requirements, ICT risk management, and reporting obligations
- ✓ **Incident Response & Crisis Management** – Planning and management of cyberattacks, including communication with authorities and liability mitigation
- ✓ **Contract Drafting & Supply Chain Security** – Drafting IT service and supplier contracts in accordance with statutory cybersecurity obligations
- ✓ **Training & Empowerment** – Training executives, compliance, and IT teams on legal cybersecurity obligations and their practical implementation

Our Services

Deloitte Legal & Deloitte: As One Deloitte, we provide comprehensive advice on cybersecurity and legal matters.

- ✓ **Holistic legal and regulatory advice across the entire cybersecurity compliance chain - from risk analysis to communication with regulatory authorities**
- ✓ **Development and review of cyber governance structures and the legal framework for IT risk management**
- ✓ **Review and structuring of all legal relationships with regard to cybersecurity - from the supply chain to cloud contracts to insurance solutions**

YOUR CONTACT

Dr. Söntje Julia Hilberg, LL.M.

Attorney at Law | Partner
Co-Lead, Digital Law
Email: shilberg@deloitte.de
Phone: +49 30 254683016
Mobile: +49 170 7663353

Juliane Franze

Attorney at Law | Senior Manager
Email: jfranze@deloitte.de
Phone: +49 30 254683656
Mobile: +49 151 54484834