Deloitte.
Legal

# Digital Sovereignty:
# Legal Perspective

# Dimensions of Digital Sovereignty

Digital sovereignty is a legal policy-making task—from setting the strategic course to operational implementation.

01

**Strategy**

Slide 3 →

02

**Infrastructure & Platform**

Slide 4 →

03

**Software**

Slide 5 →

04

**Data**

Slide 6 →

05

**Security & Compliance**

Slide 7 →

06

**Operations**

Slide 8 →

# 01 Strategy

Sovereignty begins with the law: Geopolitical risks and regulatory frameworks are not peripheral considerations, but rather the starting point for every sovereign strategic decision.

## Key Legal Issues

- **CLOUD Act and FISA (U.S.):** Allow foreign authorities to access data held by U.S. companies—regardless of the physical location of the data
- **AWG/AWV and the EU Screening Regulation:** Tighter investment controls restrict who is permitted to invest in critical digital technologies
- **EU AI Act, Data Act, NIS-2, DORA:** Mandatory minimum regulatory requirements that must be taken into account when selecting providers and technologies
- **Vendor lock-in as an issue under contract and competition law:** A lack of exit options legally cements dependencies
- **Geopolitical events** challenge established ecosystems and create new, sometimes still unclear compliance requirements

## Our Services

- **Legal Sovereignty Risk Analysis:** Identification of relevant legal risks by jurisdiction and technology layer
- **Development of a legally sound sovereignty strategy** with a clear vision, prioritization, and roadmap
- **Clear distinction between mandatory requirements** (regulatory compliance) **and target requirements** (strategic sovereignty goals)
- **Legal assessment** of cloud architecture and provider decisions
- **Regulatory affairs consulting** with the European Commission and national authorities

# 02 Infrastructure & Platform

Sovereign infrastructure starts with the RFP: If you want to avoid dependency, you must legally rule it out at the time the contract is signed—by setting clear requirements regarding ownership, data residency, and the ability to switch providers.

## Key Legal Issues

- **Public Procurement Law:** Embedding sovereignty requirements as transparent, traceable award criteria in tenders
- **EU Cloud Sovereignty Framework, BSI C5 Criteria, and EUCS:** Regulatory standards for comparing providers and as legally relevant minimum requirements
- **GAIA-X:** European framework for sovereign data infrastructures and certification requirements
- **Telecommunications Act (TKG) and KRITIS Regulation:** Specific requirements for critical infrastructures, including restrictions on high-risk suppliers in the 5G sector
- **Geopolitical, regulatory, and technological risks** (vendor lock-in, data access, loss of operational autonomy) as procurement criteria relevant under public procurement law

## Our Services

- **Public procurement law advice** on the legally compliant drafting of tenders with embedded sovereignty requirements
- **Drafting sovereign cloud contracts** with specific requirements regarding ownership structures (e.g., exclusively European owners, comparable requirements for subcontractors and hardware suppliers), residence and nationality of personnel deployed, clear audit, documentation, and evidence requirements, as well as exit and termination provisions and interoperability requirements under the Data Act
- **Legal support during migration and go-live:** acceptance criteria, traceability of migration steps, prevention of data transfers outside the target region, and remedies in the event of violations of sovereignty requirements

# 03 Software

Those who are unfamiliar with the license terms lose control: software sovereignty is achieved through smart contract drafting, open-source governance, and contractual exit rights—not through technical decisions alone.

## Key Legal Issues

- **Software Licensing Law:** Risks posed by proprietary licenses and restrictive terms of use that permanently tie companies to individual providers
- **Open-Source Licenses (GPL, AGPL, Apache, MIT):** Copyleft clauses can restrict the free use of a company's own developments
- **IP Law:** Copyright protection of source code, protection and commercialization of software developments
- **EU AI Act:** Requirements for software development for high-risk AI systems (Annex III)
- **Cyber Resilience Act (CRA):** Mandatory security requirements for products with digital elements throughout the entire product lifecycle
- **Dual-Use Regulation (Regulation 2021/821):** Export control laws for AI systems and security-related software

## Our Services

- **Licensing due diligence for the use of open-source software:** Identification of copyleft risks and license incompatibilities
- **Drafting of software development and license agreements with sovereignty clauses:** source code deposit, audit rights, and usage rights after the end of the contract
- **Negotiation of** contractual exit and portability rights
- **Advice** on open-source governance structures
- **Advice on export control laws** for software products and AI systems
- **IP advice** for technology companies and software manufacturers

# 04 Data

Data sovereignty is not a technical promise—it must be enforced legally: through contracts, data transfer impact assessments, and the targeted use of European data protection instruments.

## Key Legal Issues

- **GDPR:** Requirements for transfers to third countries, transfer impact assessments, Standard Contractual Clauses (SCCs), and Binding Corporate Rules (BCRs)
- **Data Act (Regulation 2023/2854):** Rights to IoT data, regulations on cloud switching, and explicit protection against access by third-country authorities to non-personal data (Art. 30 et seq.)
- **Data Governance Act:** Framework for sovereign data sharing and reuse of public datasets
- **Concentration risks and access** to data by other jurisdictions as an integral part of risk analysis
- **EU-US Data Privacy Framework:** Ongoing political stability risk that must be monitored from a legal perspective and safeguarded through contractual arrangements

## Our Services

- **Conducting** data transfer impact **assessments** (TIA), advising on data localization requirements and jurisdictional risks
- **Drafting data processing agreements and data access regulations** (Data Act and DGA compliance)
- **Development of contractual sovereignty clauses** (“Sovereignty by Contract”) that effectively preclude access by foreign authorities
- **Legal support** in implementing data encryption and access policies

# 05 Security & Compliance

Digital sovereignty without a legally enforceable security framework is not sustainable: NIS-2, DORA, and the Cyber Resilience Act make cybersecurity the personal responsibility of corporate leadership.

## Key Legal Issues

- **NIS-2 Directive:** Comprehensive risk management, security incident reporting requirements, supply chain security, and personal liability of management bodies
- **DORA:** Mandatory penetration testing (Threat-Led Penetration Testing, TLPT), ICT incident reporting obligations, and direct oversight of critical third-party ICT service providers
- **Cyber Resilience Act (CRA):** Mandatory security requirements for all products with digital elements throughout the entire product lifecycle
- **BSI C5 Criteria and EUCS:** Minimum standards for sovereign cloud services with legal implications in tenders and contracts
- **Conditions for approval and prerequisites for further outsourcing** as protective mechanisms to be enshrined in contracts
- **Sector-specific requirements** (e.g., the Hospital Future Act): Obligation to store data within the EU

## Our Services

- **Gap analyses and compliance audits** under NIS-2, DORA, the Cyber Resilience Act, BSI C5, and EUCS
- **Establishment of legal compliance frameworks** for information and cybersecurity
- **Advice on the personal liability of management bodies** and the establishment of a documented, audit-proof governance structure
- **Drafting contracts with third-party ICT service providers** while fully taking into account all regulatory security requirements
- **Legal support during certification processes** (BSI C5 certificates, EUCS certification)
- **Advice and representation** regarding reports to and proceedings with regulatory authorities following cybersecurity incidents

# 06 Operations

Sovereignty does not end with the conclusion of a contract: Even when IT services are outsourced, legal responsibility and liability remain with the company.

## Key Legal Issues

- **NIS 2 Directive:** Risk management, reporting obligations, and personal liability of management bodies
- **DORA:** Requirements for digital operational resilience, management of third-party ICT service providers, and assessment of concentration risks
- **Principle of Continued Responsibility:** The outsourcing company remains responsible for compliance with all legal requirements—legal delegation is not possible
- **KWG, MaRisk, EBA Guidelines:** Sector-specific outsourcing requirements for the financial sector
- **Art. 31 et seq. DORA:** Direct supervision of critical third-party ICT service providers by European supervisory authorities
- **Disaster recovery, failover readiness, and business continuity planning** as mandatory legal requirements

## Our Services

- **Drafting DORA-compliant contracts** with third-party **ICT service providers**, including audit, documentation, and verification obligations, as well as approval requirements for further outsourcing
- **Development of legally sound exit strategies:** Ensuring the ability to exit without disrupting business operations, without compromising regulatory compliance, and without compromising the quality of customer services
- **Identification and assessment of concentration risks** among third-party ICT service providers
- **Advice on the personal liability of management bodies** (NIS-2 management liability)
- **Support** during regulatory audits and inquiries from authorities

Deloitte.
Legal

Digital sovereignty is a legal policy-making task—from setting the strategic course to operational implementation.

***We'll guide you along this path.***

Deloitte.
Legal

## CONTACT


### Dr. Till Contzen

Attorney at Law | Partner
*Co-Lead, Digital Law*

Email: tcontzen@deloitte.de
Phone: +49 69 719188439
Mobile: +49 173 1576309

### 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




MAKING AN IMPACT THAT MATTERS since 1845