Deloitte.
Legal

Digitale Souveränität:
Rechtliche Perspektive

Dimensionen der digitalen Souveränität

Digitale Souveränität ist eine rechtliche Gestaltungsaufgabe – von der strategischen Weichenstellung bis zur operativen Umsetzung.

01

Strategie

Folie 3 →

02

Infrastruktur & Plattform

Folie 4 →

03

Software

Folie 5 →

04

Daten

Folie 6 →

05

Sicherheit & Compliance

Folie 7 →

06

Betrieb

Folie 8 →

01 Strategie

Souveränität beginnt mit dem Recht: Geopolitische Risiken und regulatorische Rahmenbedingungen sind keine Randbedingungen, sondern Ausgangspunkt jeder souveränen Strategieentscheidung.

Rechtliche Kernthemen

- **CLOUD Act und FISA (USA):** Ermöglichen ausländischen Behörden den Zugriff auf Daten bei US-Unternehmen – unabhängig vom physischen Speicherort
- **AWG/AWV und EU-Screening-Verordnung:** Verschärfte Investitionskontrolle schränkt ein, wer in kritische Digitaltechnologien investieren darf
- **EU AI Act, Data Act, NIS-2, DORA:** Verbindliche regulatorische Mindestanforderungen, die bei der Anbieter- und Technologiewahl zwingend zu berücksichtigen sind
- **Vendor Lock-in als Vertrags- und Wettbewerbsrechtsthema:** Fehlende Exit-Optionen zementieren Abhängigkeiten rechtlich
- **Geopolitische Ereignisse** fordern etablierte Ökosysteme heraus und schaffen neue, teils noch unklare Compliance-Anforderungen

Unsere Services

- **Rechtliche Souveränitäts-Risikoanalyse:** Identifikation relevanter Rechtsrisiken nach Jurisdiktion und Technologieschicht
- **Entwicklung einer rechtlich fundierten Souveränitätsstrategie** mit klarem Zielbild, Priorisierung und Roadmap
- **Klare Trennung von Muss-Anforderungen** (regulatorische Compliance) **und Soll-Anforderungen** (strategische Souveränitätsziele)
- **Rechtliche Bewertung** von Cloud-Architektur- und Anbieterentscheidungen
- **Regulatory-Affairs-Beratung** gegenüber EU-Kommission und nationalen Behörden

02 Infrastruktur & Plattform

Souveräne Infrastruktur beginnt bei der Ausschreibung: Wer Abhängigkeit vermeiden will, muss sie bereits beim Vertragsschluss rechtlich ausschließen – durch klare Anforderungen an Eigentümerschaft, Datenresidenz und Anbieterwechsel.

Rechtliche Kernthemen

- **Vergaberecht:** Souveränitätsanforderungen als transparente, nachvollziehbare Zuschlagskriterien in Ausschreibungen verankern
- **EU Cloud Sovereignty Framework, BSI C5-Kriterien und EUCS:** Regulatorische Standards zur Vergleichbarkeit von Anbietern und als rechtlich relevante Mindestanforderungen
- **GAIA-X:** Europäischer Rahmen für souveräne Dateninfrastrukturen und Zertifizierungsanforderungen
- **TKG und KRITIS-Regulierung:** Spezifische Anforderungen an kritische Infrastrukturen, einschließlich der Beschränkung von Hochrisikolieferanten im 5G-Bereich
- **Geopolitische, regulatorische und technologische Risiken** (Vendor Lock-in, Datenzugriff, Verlust operativer Autonomie) als vergaberechtlich relevante Beschaffungskriterien

Unsere Services

- **Vergaberechtliche Beratung** zur rechtssicheren Gestaltung von Ausschreibungen mit verankerten Souveränitätsanforderungen
- **Gestaltung souveräner Cloud-Verträge** mit konkreten Anforderungen an Eigentumsverhältnisse (z. B. ausschließlich europäische Eigentümer, vergleichbare Anforderungen an Subunternehmer und Hardwarelieferanten), Wohnsitz und Nationalität des eingesetzten Personals, klare Audit-, Dokumentations- und Nachweispflichten sowie Exit- und Kündigungsregelungen und Interoperabilitätsvorgaben nach dem Data Act
- **Rechtliche Begleitung bei Migration und Go-Live:** Abnahmekriterien, Nachvollziehbarkeit der Migrationsschritte, Vermeidung von Datentransfers außerhalb der Zielregion, Lösungsrechte bei Verstößen gegen Souveränitätsanforderungen

03 Software

Wer die Lizenzbedingungen nicht kennt, verliert die Kontrolle: Softwaresouveränität entsteht durch kluge Vertragsgestaltung, Open-Source-Governance und vertragliche Exit-Rechte – nicht durch technische Entscheidungen allein.

Rechtliche Kernthemen

- **Softwarelizenzrecht:** Risiken durch proprietäre Lizenzen und restriktive Nutzungsbedingungen, die Unternehmen dauerhaft an einzelne Anbieter binden
- **Open-Source-Lizenzen (GPL, AGPL, Apache, MIT):** Copyleft-Klauseln können die freie Verwertbarkeit eigener Entwicklungen einschränken
- **IP-Recht:** Urheberrechtlicher Schutz von Quellcode, Schutz und Verwertung von Softwareentwicklungen
- **EU AI Act:** Anforderungen an Softwareentwicklung für hochriskante KI-Systeme (Anhang III)
- **Cyber Resilience Act (CRA):** Verbindliche Sicherheitsanforderungen für Produkte mit digitalen Elementen über den gesamten Produktlebenszyklus
- **Dual-Use-Verordnung (VO 2021/821):** Exportkontrollrecht bei KI-Systemen und sicherheitsrelevanter Software

Unsere Services

- **Lizenzrechtliche Due Diligence bei Open-Source-Einsatz:** Identifikation von Copyleft-Risiken und Lizenzinkompatibilitäten
- **Gestaltung von Softwareentwicklungs- und Lizenzverträgen mit Souveränitätsklauseln:** Quellcode-Hinterlegung, Auditrechte, Nutzungsrechte nach Vertragsende
- **Verhandlung** vertraglicher Exit- und Portabilitätsrechte
- **Beratung** zu Open-Source-Governance-Strukturen
- **Exportkontrollrechtliche Beratung** für Softwareprodukte und KI-Systeme
- **IP-Beratung** für Technologieunternehmen und Softwarehersteller

04 Daten

Datensouveränität ist kein technisches Versprechen – sie muss rechtlich durchgesetzt werden: durch Verträge, Transfer-Folgenabschätzung und den gezielten Einsatz europäischer Datenschutzinstrumente.

Rechtliche Kernthemen

- **DSGVO:** Anforderungen an Drittlandtransfers, Transfer Impact Assessments, Standardvertragsklauseln (SCC) und Binding Corporate Rules (BCR)
- **Data Act (VO 2023/2854):** Rechte an IoT-Daten, Regelungen zum Cloud-Switching und expliziter Schutz vor dem Zugriff drittstaatlicher Behörden auf nicht-personenbezogene Daten (Art. 30 ff.)
- **Data Governance Act:** Rahmen für souveräne Datenvermittlung und Weiterverwendung öffentlicher Datensätze
- **Konzentrationsrisiken und Zugriffsmöglichkeiten** auf Daten durch andere Jurisdiktionen als integraler Bestandteil der Risikoanalyse
- **EU-US Data Privacy Framework:** Fortlaufendes politisches Stabilitätsrisiko, das rechtlich beobachtet und vertraglich abgesichert werden muss

Unsere Services

- **Durchführung von Datentransfer-Folgenabschätzungen** (Transfer Impact Assessments), Beratung zu Datenlokalisierungsanforderungen und jurisdiktionellen Risiken
- **Gestaltung von Datenverarbeitungsverträgen und Datenzugangsregelungen** (Data Act- und DGA-Compliance)
- **Entwicklung vertraglicher Souveränitätsklauseln** (Sovereignty by Contract), die den Zugriff durch fremde Behörden wirksam ausschließen
- **Rechtliche Begleitung** bei der Einführung von Datenverschlüsselungs- und Zugriffsrichtlinien

05 Sicherheit & Compliance

Digitale Souveränität ohne rechtlich durchsetzbaren Sicherheitsrahmen ist nicht tragfähig: NIS-2, DORA und der Cyber Resilience Act machen Cybersicherheit zur persönlichen Verantwortung der Unternehmensleitung.

Rechtliche Kernthemen

- **NIS-2-Richtlinie:** Umfassendes Risikomanagement, Meldepflichten bei Sicherheitsvorfällen, Lieferkettensicherheit und persönliche Haftung der Leitungsorgane
- **DORA:** Verpflichtende Penetrationstests (Threat Led Penetration Testing, TLPT), IKT-Vorfallsmeldepflichten und direkte Aufsicht über kritische IKT-Drittdienstleister
- **Cyber Resilience Act (CRA):** Verbindliche Sicherheitsanforderungen für alle Produkte mit digitalen Elementen über den gesamten Produktlebenszyklus
- **BSI C5-Kriterien und EUCS:** Mindeststandards für souveräne Cloud-Dienste mit rechtlicher Relevanz in Ausschreibungen und Verträgen
- **Zustimmungsvorbehalte und Voraussetzungen für Weiterverlagerungen** als vertraglich zu verankernde Schutzmechanismen
- **Sektorspezifische Anforderungen** (z. B. Krankenhauszukunftsgesetz): Pflicht zur Datenhaltung innerhalb der EU

Unsere Services

- **Gap-Analysen und Compliance-Prüfungen** unter NIS-2, DORA, Cyber Resilience Act, BSI C5 und EUCS
- **Aufbau rechtlicher Compliance-Strukturen** für Informations- und Cybersicherheit
- **Beratung zur persönlichen Haftungssituation der Leitungsorgane** und Aufbau einer dokumentierten, revisionssicheren Governance-Struktur
- **Vertragsgestaltung mit IKT-Drittdienstleistern** unter vollständiger Berücksichtigung aller regulatorischen Sicherheitsanforderungen
- **Rechtliche Begleitung bei Zertifizierungsverfahren** (BSI C5-Testate, EUCS-Zertifizierung)
- **Beratung und Vertretung** bei Behördenmeldungen und -verfahren nach Cybersicherheitsvorfällen

06 Betrieb

Souveränität endet nicht am Vertragsschluss: Auch bei ausgelagerten IT-Diensten bleibt die rechtliche Verantwortung und die Haftung beim Unternehmen.

Rechtliche Kernthemen

- **NIS-2-Richtlinie:** Risikomanagement, Meldepflichten und persönliche Organhaftung der Leitungsorgane
- **DORA:** Anforderungen an digitale operationale Resilienz, IKT-Drittdienstleister-Management und Bewertung von Konzentrationsrisiken
- **Grundsatz der fortbestehenden Verantwortung:** Das auslagernde Unternehmen bleibt für die Einhaltung aller gesetzlichen Anforderungen verantwortlich – eine rechtliche Delegation ist nicht möglich
- **KWG, MaRisk, EBA-Leitlinien:** Sektorspezifische Auslagerungsanforderungen für den Finanzsektor
- **Art. 31 ff. DORA:** Direkte Aufsicht über kritische IKT-Drittdienstleister durch die europäischen Aufsichtsbehörden
- **Disaster Recovery, Failover-Bereitschaft und Kontinuitätsplanung** als verbindliche rechtliche Anforderungen

Unsere Services

- **Gestaltung DORA-konformer IKT-Drittdienstleisterverträge** mit Audit-, Dokumentations- und Nachweispflichten sowie Zustimmungsvorbehalten bei Weiterverlagerungen
- **Entwicklung rechtlich belastbarer Ausstiegsstrategien:** Sicherstellung der Ausstiegsfähigkeit ohne Unterbrechung des Geschäftsbetriebs, ohne Beeinträchtigung der regulatorischen Compliance und ohne Einschränkung der Qualität von Kundendienstleistungen
- **Ermittlung und Bewertung von Konzentrationsrisiken** bei IKT-Drittdienstleistern
- **Beratung zur persönlichen Haftungssituation der Leitungsorgane** (NIS-2 Organhaftung)
- **Begleitung** bei aufsichtsrechtlichen Prüfungen und Behördenanfragen

Deloitte.
Legal

Digitale Souveränität ist eine rechtliche Gestaltungsaufgabe – von der strategischen Weichenstellung bis zur operativen Umsetzung.

Wir begleiten Sie auf diesem Weg.

Deloitte.
Legal

KONTAKT

Dr. Till Contzen

Rechtsanwalt I Partner
Co-Lead Digital Law

E-Mail: tcontzen@deloitte.de
Phone: +49 69 719188439
Mobile: +49 173 1576309

Dr. Söntje Julia Hilberg, LL.M.

Rechtsanwältin I Partner
Co-Lead Digital Law

E-Mail: shilberg@deloitte.de
Phone: +49 30 254683016
Mobile: +49 170 7663353

MAKING AN IMPACT THAT MATTERS since 1845