TaylorWessing

DIGITAL LEGAL
ACADEMY 2026

Die neue digitale Ordnung im Brennpunkt

Digital Sovereignty: Zwischen globaler Vernetzung und regionaler Kontrolle

Katrin Hellwig, Sandra Hattwig & Dr. Carsten Schulz | 15. April 2026

Sessions 2026

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

#1	**Digital Sovereignty: Zwischen globaler Vernetzung und regionaler Kontrolle** Katrin Hellwig, Sandra Hattwig & Dr. Carsten Schulz am 15. April 2026
#2	**Digital Fairness: Der EU-Ansatz zu Dark Patterns, Personalisierung und digitalem Verbraucherschutz** Christine Steffen, Nathalie Koch & Thanos Rammos am 22. April 2026
#3	**Digital Resilience: Schutzschild gegen Cyberkriminelle** Dr. Judith Nink, Wiebke Reuter & Dr. Paul Voigt am 29. April 2026
#4	**Digital Responsibility: Wer übernimmt die „digitale Verantwortung“?** Magda Grünewald, Maximilian Höving & Dr. Benedikt Rohrßen am 6. Mai 2026
#5	**Panel-Diskussion: Digital Geopolitics** Prof. Dr. Rolf Schwartmann, Prof. Dr. Dieter Kugelmann, Svenja-Ariane Maucher & Dr. Axel Freiherr von dem Bussche am 13. Mai 2026

Speaker

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Dr. Carsten Schulz

Partner, Taylor Wessing

Sandra Hattwig

Senior Associate, Taylor Wessing

Katrin Hellwig

Senior Legal Counsel, Arvato Systems

Agenda

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

DIGITAL LEGAL
ACADEMY 2026
by TaylorWessing

1 Digitale Souveränität – Erste Einordnung

Definition und Einordnung

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Digitale Souveränität

ist kein universell anerkannter Begriff – wird kontextabhängig von verschiedenen Institutionen mit unterschiedlicher Schwerpunktsetzung verwendet.

Grundsätzliches Verständnis:

> Die Fähigkeit von Individuen, Unternehmen und Staaten, digitale Infrastrukturen, Daten und Technologien selbstbestimmt und unabhängig zu kontrollieren, zu gestalten und zu nutzen.

Digitale Souveränität aus verschiedenen Perspektiven

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Individuelle IT-Nutzer

- IT erfolgreich, sicher und rechtssicher **nutzen** sowie **angemessen Zugang** zu digitalen Ressourcen haben
- Selbstbestimmt über Herausgabe, Erfassung, Speicherung, Nutzung und Verarbeitung **eigener Daten** entscheiden

Institutionelle IT-Nutzer

- Alle **Aspekte individueller digitaler Souveränität** übertragen auf die gesamte Institution
- Schutz sensibler Daten und selbstbestimmter Zugriff auf neuste Technologien als **wirtschaftlicher Erfolgsfaktor**

IT-Hersteller und Service Provider

- Fähigkeit, angestrebte Produkte und Dienstleistungen zu realisieren (**Entwurfs- und Produktionssouveränität)**
- Möglichkeit im fairen Wettbewerb auf den Zielmärkten bestehen zu können (**Marktsouveränität**)

Gesamtgesellschaft

- Fähigkeit, IT-Komponenten **selbst zu entwickeln und digital souverän** zu agieren; **Reduzierung von Abhängigkeiten**
- **Schutz** vor äußeren wirtschaftlichen und politischen Eingriffen
- **Stabilität** im digitalen Bereich/ bei Einsatz von IT

Quelle: Goldacker, Digitale Souveränität, ÖFIT/ Frauenhofer FOKUS, Berlin 2017.

Verschiedene Dimensionen der Digitalen Souveränität

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Betriebliche Souveränität

- Fähigkeit, digitale Systeme und Prozesse **stabil und unabhängig zu betreiben**
- Vermeidung von kritischen Lock-ins und Sicherstellung der **Betriebsfähigkeit**

Technische Souveränität

- Zugriff auf und Kontrolle über **Schlüsseltechnologien** (Cloud, KI, Security)
- Fähigkeit, Technologien bewusst **auszuwählen, zu kombinieren** und **weiterzuentwickeln**

Datensouveränität

- Fähigkeit eigene Daten zu **besitzen**, **kontrollieren**, zu **schützen** und ihre Nutzung zu bestimmen
- **Transparenz** über Datenflüsse und sichere Austauschbarkeit sicherstellen

Juristische Souveränität

- Sicherstellung **Compliance mit europäischen und nationalen Vorgaben**
- **Minimierung von Konflikten** mit extraterritorialen Gesetzen anderer Staaten

Quelle: Zillmann/Ganowski, Lünendonk-Studie: Digitale Souveränität – Vom Risiko zur Resilienz, Lünendonk & Hossenfelder GmbH, Mindelheim 2026.

Kernelemente

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Selbstbestimmung	Kontrolle über Daten & technischer Infrastruktur	Unabhängigkeit ohne Abschottung
Entscheidungs- und Wahlfreiheit für oder gegen eine Technologie	Schutz vor fremdem Zugriff und Einflussnahme	Keine Autokratie, sondern bewusste Steuerung von Abhängigkeiten

Handlungsfähigkeit

Bestehende Digitale Abhängigkeit in der Wirtschaft

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Repräsentative Befragung von 603 Unternehmen aller Branchen in Deutschland ab 20 Beschäftigten:

96%

der deutschen Unternehmen beziehen digitale Services & Technologien aus dem Ausland

90%

unter den Importeuren digitaler Technologien und Leistungen sehen sich als „stark“ oder „eher“ abhängig von ausländischen Partnern

60%

erwarten in den nächsten 5 Jahren eine steigende Importabhängigkeit Deutschlands

Quelle: Bitkom e.V. (Hrsg.), Digitale Souveränität – Wie abhängig ist unsere Wirtschaft?, 2025.

Hauptgründe für Digitale Souveränität

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

1. Geopolitische Resilienz & Strategische Autonomie

- Technische Dominanz einzelner Länder wird gezielt als geopolitisches Druckmittel eingesetzt
- Souveräne Infrastruktur als Antwort auf fragmentierte, rivalisierende Weltordnung

2. Vendor Lock-In

- **Übermäßige Abhängigkeiten** in der IT-Lieferkette gefährden die Fähigkeit von Unternehmen, **technologische Entscheidungen unabhängig** zu treffen

Main Drivers

3. Datenschutz & Rechtssicherheit

- Strukturelles und extraterritoriales **Spannungsverhältnis** zum europäischen Datenschutzrecht (DSGVO)
- Beginnende **rechtliche Regulierung** Digitaler Souveränität

4. Wettbewerbsfähigkeit

- Digitale Souveränität wirkt sich positiv auf **Kunden-beziehungen** sowie **Kosten- & Effizienzpotenziale** aus
- Befähigt Unternehmen, **Risiken aktiv zu steuern**, statt ihnen passiv ausgeliefert zu sein

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

2 Digitale Souveränität – Der Europäische Rahmen

Der Europäische Rahmen

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Das Cloud Sovereignty Framework der EU-Kommission definiert Souveränitätsziele

Vergleich verschiedener europäischer Ansätze

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Merkmal	Deutschland	Frankreich	Nordics / Baltikum
Primärer Fokus	Rechtssicherheit & Verwaltung	Wirtschaftskraft & Champions	Agilität & Bürgerservice
Haltung zu US-Tech	Kritisch / Distanziert	Konkurrenzorientiert	Pragmatisch / Sicherheitsorientiert
Lösungsweg	Open Source & Regulierung	Industriepolitik & Subventionen	Digital-First & Verschlüsselung
Leitmotiv	„Digitale Selbstbestimmung“	„Strategische Autonomie“	„Digital Resilience“

Der französische SecNumCloud Ansatz

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Bereich	Kernregelung (SecNumCloud 3.2)	Bedeutung für die Souveränität
Rechtlicher Schutz	**Immunität gegen extraterritoriale Gesetze:** Der Anbieter muss nachweisen, dass außereuropäische Gesetze keinen Zugriff auf die Daten erlauben.	Verhindert, dass ausländische Behörden ohne EU-Rechtsgrundlage auf Daten zugreifen können.
Eigentumsverhältnisse	**Beschränkung ausländischer Anteile:** Nicht-EU-Unternehmen dürfen max. 24% der Anteile einzeln und 39% kollektiv halten.	Stellt sicher, dass die strategische Kontrolle über den Cloud-Anbieter in europäischer Hand bleibt.
Datenstandort	**Lokalität:** Die Server müssen physisch in der EU stehen; der Betrieb und Support müssen von EU-Boden aus erfolgen.	Physische Kontrolle über die Infrastruktur und Einhaltung europäischer Datenschutzstandards.
Personal	**Sicherheitsüberprüfung:** Administratoren mit hohen Privilegien müssen strengen Hintergrundchecks unterzogen werden.	Schutz vor Spionage oder Sabotage durch Innentäter oder fremde Geheimdienste.
Technik	**Starke Isolation & Verschlüsselung:** Mandantentrennung auf höchstem Niveau und MFA für alle administrativen Zugänge.	Technischer Schutz der Vertraulichkeit, selbst wenn die Hardware-Ebene angegriffen wird.
Vertrag / Ausstieg	**Reversibilität:** Verpflichtende Klauseln zur Datenrückführung und Löschung bei Vertragsende.	Vermeidung von **Vendor Lock-in**; die Souveränität, den Anbieter jederzeit wechseln zu können.

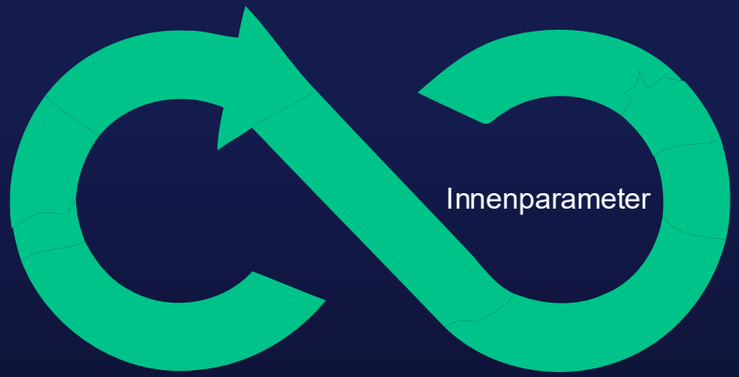
DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

3 Digitale Souveränität in der Praxis

Digitale Souveränität in der Praxis

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Digitale Souveränität als permanenter Abwägungsprozess zwischen verschiedenen Zielen



Außenbedingungen

- Tiefe der Wertschöpfung
- Skalierungseffekte vs. Klumpenrisiko
- Innovation vs. Follower
- Sinnvolle Bevorratung

- Resilienz bei unvorhersehbaren Szenarien
- Physikalische Sicherheit
- IT-Sicherheit bei Hardware und Software
- Zugriffsmöglichkeiten durch Dritte
- Geopolitische Resistenz und Dokumentation

- Attraktivität des Service-Portfolios
- Kundenfreundlichkeit im Nutzen und Preis
- Skalierungs- und Betriebsfähigkeit
- Wettbewerbsfähigkeit/-überlegenheit
- Attraktivität

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

4 Besonders betroffene Rechtsträger

Digitale Souveränität in der Verwaltung

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

SUMMIT ON EUROPEAN DIGITAL SOVEREIGNTY

Verantwortung für Deutschland

Koalitionsvertrag zwischen CDU, CSU und SPD

21. Legislaturperiode

Deutschland-Stack

Gipfel zur europäischen digitalen Souveränität

Startschuss für eigenständigeres Europa

bundesregierung.de

Weg von Microsoft: Abgeordnete fordern digitale Souveränität im EU-Parlament

heise.de

Die FITKO stellt vor: Die föderale Zielarchitektur für Postfach- und Kommunikationslösungen (ZaPuK)

digitale-verwaltung.de

Bundesregierung beschließt Rechenzentrumsstrategie

Wildberger: „Jedes neue Rechenzentrum stärkt unsere digitale Souveränität und Wettbewerbsfähigkeit“

bmds.bund.de

Digitale Souveränität kritischer Infrastrukturen und Industrien

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing







Energie

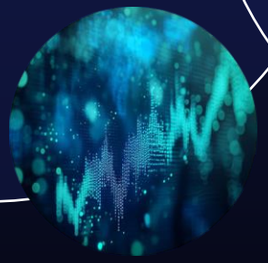
Transport

Finanzsektor

Gesundheit





Digitale Abhängigkeit als besonderes Risiko

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Verlust der eigenständigen Betriebsfähigkeit

Besondere Sichtbarkeit macht Datenverluste existenziell

Eingeschränkte Verhandlungsmacht & Steigende Kosten

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

5 Rechtlicher Rahmen

Rechtliche Anforderungen an Digitale Souveränität

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Kein deutsches „Souveränitätsgesetz“: kein zentraler gesetzlicher Ansatz, sondern Umsetzung und Ergänzung europäischer Leitplanken.
Bestehende gesetzliche Regelungen können in folgende „Souveränitätsziele“ unterteilt werden:

Daten- & Marktsouveränität (Kontrolle & Wettbewerb)	Infrastruktur- & Hardware-Souveränität	Cyber-Sicherheit & Resilienz (Operative Souveränität)
▪ DSGVO (Datenschutz-Grundverordnung) ▪ Data Act ▪ **Digital Markets Act (DMA)** ▪ **Digital Services Act (DSA)**	▪ **EU Chips Act** ▪ **eIDAS 2.0**	▪ NIS-2 ▪ **DORA (Digital Operational Resilience Act)** ▪ Cyber Resilience Act (CRA) ▪ AI Act

DSGVO – Grundlagen & Souveränitätsbezug

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Anwendungsbereich

Verarbeitung personenbezogener Daten

- Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Pereson beziehen (vgl. Art. 4 DSGVO)
- pseudonyme Daten vs. anonyme Daten
- Weiter Verarbeitungsbegriff

- Grundsätzlich nicht im Anwendungsbereich der DSGVO:
  - Betriebs- und Geschäftsgeheimnisse

Grundsätze für die Verarbeitung personenbezogener Daten

Grundsatz	Grundsätzliche Förderung aller Souveränitätsziele
Transparenz, Art. 5 1 a)	
Zweckbindung, Art. 5 1 b)	
Datenminimierung, Art. 5 1 c)	
Richtigkeit, Art. 5 1 d)	
Speicherbegrenzung, Art. 5 1 e)	
Integrität und Vertraulichkeit, Art. 5 1 f)	
Rechenschaftspflicht, Art. 5 (2)	

DSGVO – AVV als Souveränitätsvehikel und bereichsspezifische Anforderungen

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Auftragsverarbeitungsvertrag (AVV), Art. 28

- Festlegung Verarbeitungsort
- Umgang mit Fernzugriffen
- Weisungsgebundenheit
- Ausschluss von „Behördenzugängen“ aufgrund außereuropäischer Jurisdiktion – z.B. CLOUD Act, FISA Section 702
- Anforderungen der Art. 44ff. DSGVO
- Unterauftragnehmer
- Technische – und organisatorische Maßnahmen (z.B. Schlüsselmanagement BYOK/ HYOK)

→ **Vehikel für Souveränitätsanforderungen**

Bereichsspezifische Anforderungen

- Beispiel: Sozialgesetzliche Anforderungen
- § 80 SGB X
- § 393 SGB V

- Zwingende Anforderungen an Datenverarbeitungsort
- Zwingende Anforderung an Vorhandensein von Testaten / Zertifikaten: BSI C 5 / ISO 27001

EU Data Act (VO 2023/2854)

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

In Kraft seit dem
11. Januar 2024

In Deutschland verbindlich anwendbar seit dem
12. September 2025

Deutsches Durchführungsgesetz (**DADG**) am **26. März 2026** vom Bundestag verabschiedet

Ziel

- Förderung der Datenverfügbarkeit
- Abbau von Datenmonopolen
- Stärkung der Nutzerrechte

→ Stärkung der Datensouveränität Europas

Regelungsbereiche

- IoT-Produkte und damit verbundene Dienste
- Datenzugangsrecht der öffentlichen Hand
- Datenverarbeitungsdienste
- Internationaler Datenverkehr
- Smart Contracts

EU Data Act (VO 2023/2854)
Regelung der digitalen Souveränität

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Datensouveränität: Kontrolle über Daten

- Produktdaten und verbundene Dienstdaten müssen für den Nutzer **leicht zugänglich** sein (Art. 3, 4)
- Datenweitergabe an Drittanbieter auf Wunsch des Nutzers (Art. 5)
- **‘Data Access by Design’** ab 12. September 2026

Infrastrukturelle Souveränität: Cloud Switching & Kein Lock-In

- Anbieter von Datenverarbeitungsdiensten müssen **Wechselhindernisse beseitigen** und Kunden den Wechsel erleichtern (Art. 23)
- Ermäßigung bzw. Verbot von **Wechselentgelten** (Art. 29)

Wirtschaftliche Souveränität: Faire Verträge

- **Schutz** vor einseitig benachteiligenden Vertragsklauseln bezüglich Datennutzung (Art. 13)
- Besonderer Schutz für KMU

Staatliche Souveränität: Behördlicher Zugang in Krisenlagen

- Pflicht privater Unternehmen zur **Datenweitergabe an Behörden in Notlagen** (Art. 14)
- Sichert staatliche Handlungsfähigkeit ohne allgemeine Datenabgabepflicht

NIS 2 Richtlinie / NIS 2 UmsuCG/ Neufassung BSIG

- In Kraft seit 6. Dezember 2025
- Deutlich erweiterter Kreis betroffene Organisationen – Wesentliche / Wichtige Einrichtungen
- Risikomanagement
- Sicherheits- und Abhängigkeitskontrolle in der Lieferkette
- Meldepflichten bei Sicherheitsvorfällen – mehrstufiges Verfahren

Cyber Resilience Act

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

- Schrittweises Inkrafttreten bis 2027

- Digitale Souveränität adressiert durch:

  - Reduzierung von Abhängigkeiten durch Mindeststandards: Der CRA etabliert verbindliche Sicherheitsanforderungen für alle Produkte mit digitalen Elementen. Dies verhindert, dass unsichere Hardware oder Software aus Drittstaaten die europäische Infrastruktur schwächt und macht Europa unabhängiger von minderwertigen Technologieträgern.

  - Stärkung der Lieferkettentransparenz (SBOM): Durch die verpflichtende Einführung einer Software-Stückliste (Software Bill of Materials) erhalten europäische Unternehmen und Behörden volle Kontrolle und Wissen über die Bestandteile ihrer digitalen Werkzeuge. Das ermöglicht eine eigenständige Risikobewertung und schnelle Reaktion bei Schwachstellen.

  - Marktortprinzip: außereuropäische Anbieter unterliegen denselben rechtlichen Anforderungen.

EU-AI Act (VO 2024/1689)

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Weltweit erste umfassende KI-Regulierung

In Kraft seit 1. August 2024 und wird bis zum 2. August 2027 schrittweise vollständig wirksam

Risikobasierter Ansatz: 4 Risikoklassen

Unannehmbares Risiko – Verboten

Hohes Risiko – Streng reguliert

Begrenztes Risiko – Transparenzpflichten

Minimales Risiko – Keine Pflichten

+ zusätzliche Regelungen für General Purpose AI (GPAI)

Ziel

Herstellung und Erhaltung eines europäischen Kontrollanspruchs über KI-Systeme und ihre Auswirkungen

EU-AI Act (VO 2024/1689)
Regelung der digitalen Souveränität

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Datensouveränität: Kontrolle über KI-Datenbasis

- **Art. 10 –** Umfangreiche Datenverwaltungspflichten bei Hochrisiko-KI-Systeme
- **Art. 11, 12, 13 –** Technische Dokumentation und Transparenz bei Hochrisiko-KI-Systemen
- **Art. 53 Abs. 1 lit. d –** GPAI-Transparenz bei Trainingsdaten

Regulierungssouveränität

- **Art. 2 Abs. 1 –** Marktortprinzip
- **Art. 57 –** Nationale KI-Reallabore

Persönliche Souveränität: Schutz individueller Selbstbestimmung

- **Art. 5 – Verbotene KI-Praktiken**
  - Manipulative Verhaltenssteuerung (lit. a,b)
  - Staatliches Social Scoring (lit. c)
  - Biometrische Massenüberwachung (lit. g, h)

Souveränität durch Cybersicherheit

- **Art. 15 –** Verpflichtung zur Genauigkeit, Robustheit und Cybersicherheit bei Hochrisiko-KI
- **Art. 55 –** Cybersicherheitspflichten bei GPAI mit systematischem Risiko

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

6 Digitale Souveränität in der Verwaltung

Digitale Souveränität in der Verwaltung

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

- Umsetzung der Souveränitätsziele über allgemeine Regelungen DSGVO, Data Act, NIS-2, AI-Act etc.

- Daneben bereichsspezifische Europäische Regelungen sowie nationale Regelungen, die insbesondere auch die Förderung von Open Source Software betreffen:
  - Interoperable Europe Act (Verordnung (EU) 2024/903): Verpflichtet Verwaltungen zur grenzüberschreitenden Zusammenarbeit und zur Nutzung gemeinsamer Standards. Sie fördert explizit Open-Source-Lösungen, um die Wiederverwendbarkeit von Software in der EU zu erhöhen.
  - E-Government-Gesetz: Die Bundesbehörden sind nun gesetzlich verpflichtet, bei der Beschaffung oder Entwicklung von Software vorrangig Open-Source-Lösungen zu prüfen und einzusetzen.
  - Vergaberechtsmoderniserungsgesetz: Im Windschatten des Vegaberechtsmodernisierungsgesetzes wurden die EVB-IT umfassend überarbeitet und um Open Source Regelungen ergänzt.

- Souveränitätsziele: Vermeidung von Vendor Lock-ins, Transparenz, Stärkung des lokalen IT-Ökosystems, Langfristige Verfügbarkeit

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

7 Unternehmens-Check

Unternehmens-Check

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing

Strategische Ambition: Welchen Grad an strategischer Handlungsfähigkeit streben wir für unsere Kernprozesse an, um die wirtschaftliche Stabilität zu sichern, ohne dabei unsere Innovationskraft durch zu starre Eigenentwicklungen zu bremsen?

Rechtlicher Schutzraum: In welchem Maße muss unsere IT-Infrastruktur rechtlich und finanziell im EU-Ökosystem verankert sein, um uns wirksam vor dem Zugriff fremder Behörden und externen Rechtsansprüchen zu isolieren?

Wirtschaftliche Abwägung: Sind wir bereit, eine „Souveränitäts-Prämie“ (höhere Initialkosten oder Aufwand) zu zahlen, um langfristig die Wettbewerbsfähigkeit durch Unabhängig-keit von Monopolanbietern zu sichern?

Betriebliche Resilienz: Welche technologischen Kernkompetenzen müssen wir zwingend im eigenen Haus (oder im regionalen Verbund) vorhalten, um auch bei geopolitischen Verwerfungen handlungsfähig zu bleiben?

Daten- & KI-Autonomie: Wie viel Eigenkontrolle über unsere Datenbestände und KI-Modelle ist für unser Zielbild zwingend erforderlich, und in welchen unkritischen Bereichen akzeptieren wir die Kontrolle durch Drittanbieter?

Technologische Offenheit: Welchen Stellenwert nehmen Open Source und offene Standards in unserer Zielarchitektur ein, um sicherzustellen, dass wir Systeme jederzeit ohne technologischen Lock-in auditieren oder migrieren können?

Transparenz der Lieferkette: Wie hoch ist unser Anspruch an die geografische Herkunft und die Transparenz der IT-Lieferkette für unsere kritischen Infrastrukturen?

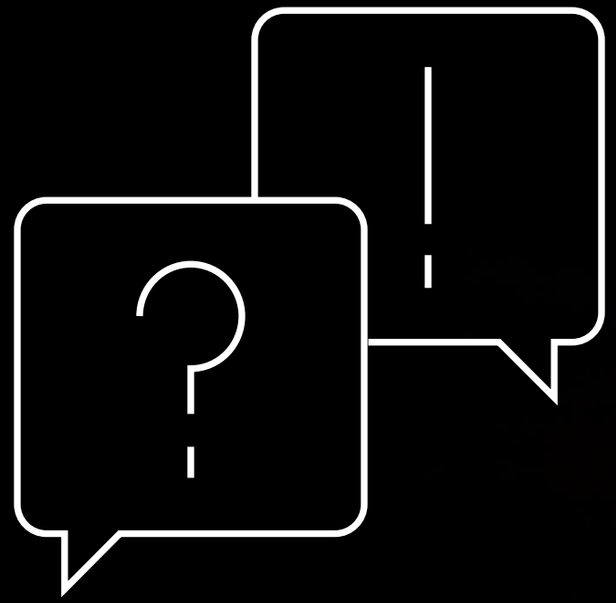
Sicherheits-Hoheit: Inwieweit sieht unser Zielbild vor, dass Sicherheitsoperationen und Compliance-Verpflichtungen ausschließlich unter unserer direkten Kontrolle innerhalb der EU verbleiben?

Nachhaltigkeits-Souveränität: Betrachten wir die Unabhängigkeit bei Energieverbrauch und die Resilienz gegenüber Rohstoffknappheit als integralen Bestandteil unserer digitalen Souveränitätsstrategie?

Interoperabilitäts-Check: Wo gewichten wir die Fähigkeit zur globalen Vernetzung und nahtlosen Zusammenarbeit mit Partnern bewusst höher als die maximale digitale Abkapselung?

Vielen Dank für eure Aufmerksamkeit

DIGITAL LEGAL ACADEMY 2026
by TaylorWessing



Q&A

TaylorWessing

DIGITAL LEGAL ACADEMY 2026

Die neue digitale Ordnung im Brennpunkt

taylorwessing.com