Deloitte.

Digitale Souveränität

Hype oder Paradigmenwechsel?

Deloitte Legal Webcast | 17. Juni 2026

Agenda & Vorstellung der Referenten

Agenda

Vorstellung der Referenten

Begriffseinordnung: Handlungsfelder digitaler Souveränität

Rechtliche Fragen am Beispiel der Finanzindustrie

Herausforderungen bei der Beschaffung souveräner IT

Zusammenfassung

Q&A

Referenten

Dr. Till Contzen
Co-Lead Digital Law
Rechtsanwalt | Partner (Deloitte Legal)

Tel.: +49 697 1918 8439
E-Mail: tcontzen@deloitte.de

Dr. Hannes Bracht
Banking & Finance
Rechtsanwalt | Partner (Deloitte Legal)

Tel.: +49 697 1918 8432
E-Mail: hbracht@deloitte.de

Daniel Lettmayer
Technology & Transformation
Senior Specialist Lead (Deloitte GmbH)

Tel.: +49 699 7137 1176
E-Mail: dlettmayer@deloitte.de

Begriffseinordnung

Handlungsfelder digitaler Souveränität

Was bewegt Organisationen zum Handeln?

Regulatorische und technologische Risiken im Fokus der Souveränitätsdiskussionen – Geopolitik wird häufig außerhalb des direkten Einflussbereichs wahrgenommen

Souveränitäts-Trigger und Risiken im Fokus

Was bewegt Organisationen zum Handeln?

Regulatorische und technologische Risiken im Fokus der Souveränitätsdiskussionen – Geopolitik wird häufig außerhalb des direkten Einflussbereichs wahrgenommen

Souveränitäts-Trigger und Risiken im Fokus

Was bewegt Organisationen zum Handeln?

Regulatorische und technologische Risiken im Fokus der Souveränitätsdiskussionen – Geopolitik wird häufig außerhalb des direkten Einflussbereichs wahrgenommen

Souveränitäts-Trigger und Risiken im Fokus

Das Souveränitäts-Dilemma des Entscheiders

Entscheidungsträger müssen regulatorische und geopolitische Zwänge mit Transformations- und Technologie-Zielen zusammen bringen

Abwägungen

Externe Druckpunkte

Souveränität: Etablierte Ökosysteme werden durch geopolitische Ereignisse herausgefordert

Regulatorische Vorgaben: Neue, jedoch noch unklare Anforderungen für viele Branchen – Compliance durch Gesetze und Richtlinien sicherstellen.

Komplexität des Technologie-Stacks: Es geht um mehr als die Einführung eines neuen Cloud-Produkts – revisionssichere, souveräne Betriebsprozesse sind erforderlich.

Souveränitäts-Compliance

BALANCE

Wertgenerierung & Innovationskraft

Interne Prioritäten

Wertrealisierung aus Technologie-Investitionen: Möglichst schneller ROI bei ERP, Cloud, KI-Vorhaben, um Effizienzpotenziale zu nutzen.

Strategische Narrative & Marktausrichtung: Cloud-Entscheidungen beeinflussen die Marktwahrnehmung und die Dynamik im Ökosystem.

Betriebliche Resilienz & KI-Bereitschaft: KI-Fähigkeiten sichern während der digitalen und souveränen Transformation.

Souveräne Cloud-Architekturen

Souveräne Cloud-Architekturen können in vier Archetypen unterteilen werden, die unterschiedliche Anforderungen adressieren. Identifizierte Risiken werden dabei durch neue Service-Angebote der Cloud-Provider aufgegriffen.

Entstehende souveräne Cloud-Architekturen

Cloud Bereitstellungsmodelle

Private Cloud | Public Cloud | Hybrid Cloud | Community Cloud

Zentrales Management		*Dezentralisiertes Management*	
			
1 US-Hyperscaler mit souveränem EU-Angebot	**2** EU-native Cloud Service Provider	**3** Proprietäre Technologie auf Infrastruktur in EU-Eigentum	**4** Open Source Lösungen mit Infrastruktur in EU-Eigentum

Ansatz für Digitale Souveränität

Unsere Experten aus verschiedenen Bereichen – von Strategie über Beratung bis hin zu Managed Services – haben ein ganzheitliches Rahmenwerk entwickelt, das Organisationen durch die enorme Komplexität des Themas führt

Deloitte's Digital Sovereignty Framework

- Betriebs-Framework, Datenresidenz-Kontrollen, Zugriffsrichtlinien
- Disaster Recovery Strategien, Failover-Bereitschaft, Kontinuitätsplanung
- Monitoring, SLA-Durchsetzung, Incident-Response Fähigkeiten

- Ansatz und Grundlagen für das Management des Datenlebenszyklus
- Datensensitivität, Verschlüsselung, regulatorische Compliance
- Richtlinien für den Datenzugriff, die Datenfreigabe und die Interoperabilität

- Software IP, vertragliche Einschränkungen, Reversibilitätsoptionen
- Ausstiegsstrategien, Interoperabilität, cloud-native Architekturen
- Praktiken für Code-Audits, Open-Source Einsatz, DevSecOps

- Infrastrukturdesign, Platzierung von Workloads, Plattformauswahl
- Workload-Migrationsfähigkeit und souveräne Plattformen zu integrieren
- Souveränitätskonforme Rechen-, Speicher- und Netzwerkkonfigurationen

Tool zur beschleunigten Umsetzung

Um sich der Digitalen Souveränität zu nähern, nutzen wir eine Sammlung von KI-Agenten, um spezifische Anforderungen und eine Roadmap zur Umsetzung zu definieren

Deloitte’s Digital Sovereignty Navigator - SONA

Unterstützt von:

SONA

Deloitte’s KI-basiertem Sovereignty Navigator-Tool

Bewertung der unternehmensspezifischen Risiken im Zusammenhang mit Souveränität anhand unseres Frameworks für Digitale Souveränität

- **Regulatorische Treiber, Cloud-Architekturen und Lösungsansätze** der Anbieter verstehen, die Ihren Sektor prägen.
- **Kritische Workloads, Risikoszenarien** und die souveräne Basis für Ihr Unternehmen identifizieren.
- **Compliance-Anforderungen, Sicherheit und wirtschaftliche Aspekte** diskutieren – mit umsetzbaren Migrationspfaden.

Praxisbeispiele im regulierten Umfeld

Souveräne Cloud Infrastruktur für SANA-Klinikum mit STACKIT*

Sana ist ein führender deutscher Gesundheitsdienstleister mit mehr als 41.000 Beschäftigten und 46 Krankenhäusern. Sana befindet sich in einer digitalen Transformation, die durch Anforderungen für die elektronische Patientenakte getrieben ist.

Zielsetzung: Aufbau einer zusätzlichen souveränen Cloud Plattform, für kritische Dienste, im Rahmen einer bestehenden Hybrid- und Multicloud-Strategie, auf der Basis von STACKIT

Datensouveränität: Aspekte der DSGVO, BSI-C5 und Krankenhauszukunftsgesetz mit der Anforderung, Patientendaten in der EU zu belassen.

Zentrale Cloud-Plattform benötigt, um zukünftige IT-Services standortübergreifend und souverän anbieten zu können.

Aufbau einer skalierbaren Umgebung (Kubernetes Container) für den Rollout weiterer IT-Services.

Aufbau einer Partnerschaft: Partnerschaft mit STACKIT und Deloitte als Beratungspartner für Konzeption und Implementierung.

Skill-Aufbau im eigenen Haus, um die neue, souveräne Plattform langfristig eigenständig betreiben zu können.

Souveräne Cloud Infrastruktur bei einer öffentlichem europäischen Finanzinstitution unter Nutzung eines EU-Cloud Providers

Ein großes europäisches öffentliches Finanzinstitut hat seine Cloud Risiken für kritische Dienste in der U.S. Cloud angesichts geopolitischer Veränderungen neu bewertet, mit dem Ergebnis einer überarbeiteten Cloud-Strategie, um die digitale Souveränität zu stärken sowie Abhängigkeitsrisiken bei kritischen Diensten zu mindern.

Zentrale Herausforderungen:

- Die veränderte geopolitische Lage im Jahr 2025 führte zu einer erhöhten Risikoexposition im Cloud-Bereich, insbesondere aufgrund der Abhängigkeit von in den USA ansässigen Hyperscalern
- Erhöhte Risiken hinsichtlich Souveränität (Verfügbarkeit) und Anbieterabhängigkeit (Vendor-Lockin), die geschäftskritische Dienste in der U.S. Cloud betreffen
- Notwendigkeit der Ermittlung geeigneter Maßnahmen zur Risikominderung
- Prüfung alternativer Hosting- und Cloud-Service-Modelle zur Risikomitigation
- Ziel: Klarer Fahrplan zur Risikominderung sowie Definition eines Umsetzungsplan

Ergebnis:

- Identifikation betroffener kritischer Dienste und Überarbeitung der Cloud-Strategie, mit Fokus auf digitale Souveränität und Risikominderung
- Implementierung einer „Sovereign Cloud Landing Zone“ bei einem EU-nativen Cloud-Anbieter, die die Migration ausgewählter kritischer Dienste ermöglicht und Abhängigkeitsrisiken reduziert
- Reduzierte Risiken im Zusammenhang mit der Abhängigkeit von U.S.-Anbietern und verbesserte Resilienz für cloudbasierte kritische Dienste

* Deutscher Cloud Service Provider im Besitz der Schwarz Gruppe

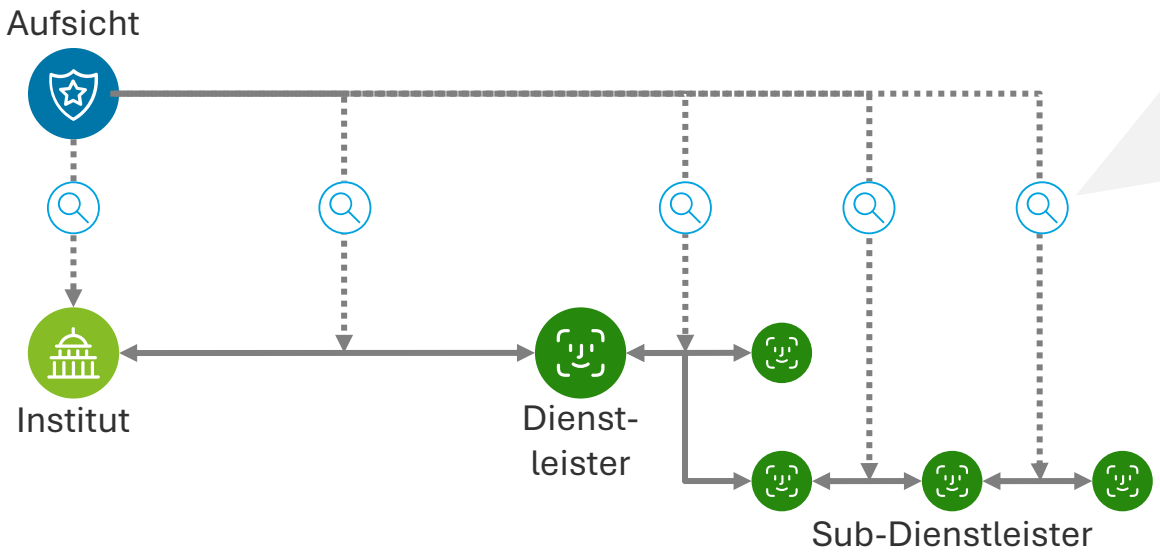
Rechtliche Fragen

am Beispiel der Finanzindustrie

Beispiel Finanzindustrie

Aufgrund der hohen Regulierungsdichte und gesamtwirtschaftlichen Bedeutung ist die Diskussion von digitaler Souveränität in der Finanzindustrie von besonderer Bedeutung.

Grundprinzip der Beaufsichtigung im digitalen Umfeld



Zentrale Regelungsmechanismen im Banken-bereich

- Kreditwesengesetz („KWG“)
- Digital Operational Resilience Act („DORA“)
- Leitlinien zu Auslagerungen der European Banking Authority („EBA“)
- Mindestanforderungen an das Risikomanagement („MaRisk“) der Bundesanstalt für Finanzdienstleistungsaufsicht („BaFin“)
- Aufsichtsmitteilung zu Auslagerungen an Cloud-Anbietern der BaFin
- Leitfaden zur Auslagerung von Cloud-Diensten an Cloud-Anbieter der Europäischen Zentralbank („EZB“)

Beispiel Finanzindustrie

„Digitale Souveränität“ selbst ist kein (bank-)aufsichtsrechtlicher Begriff, aber eine Reihe von Anforderungen zahlt auf die digitale Souveränität und bietet Anknüpfungspunkte für eine best practice auch im unregulierten Bereich.

Beispielhafte Anforderungen an vertragliche Regelungen, Risikoanalyse und Exit

„Das Institut bleibt bei einer Auslagerung für die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen verantwortlich.“

„Mit Blick auf Weiterverlagerungen sind möglichst Zustimmungsvorbehalte des auslagernden Instituts oder konkrete Voraussetzungen, wann Weiterverlagerungen einzelner Arbeits- und Prozessschritte möglich sind, im Auslagerungsvertrag zu vereinbaren.“

„Die Auslagerungsvereinbarung sollte die Übertragung der ausgelagerten Funktion an einen anderen Dienstleister oder ihre Reintegration in das Institut oder Zahlungsinstitut ermöglichen. Zu diesem Zweck sollten in der schriftlichen Auslagerungsvereinbarung folgende Regelungen enthalten sein: …“

„Im Rahmen der Risikoanalyse soll grundsätzlich Folgendes betrachtet werden: … Konzentrationsrisiken … Zugriffsmöglichkeiten auf Daten durch andere Jurisdiktionen …“

„Bei der Ermittlung und Bewertung der … genannten Risiken berücksichtigen Finanzunternehmen …:
a) Verträge mit einem IKT-Drittdienstleister, der nicht ohne Weiteres ersetzbar ist; oder
b) mehrfache vertragliche Vereinbarungen … mit demselben IKT-Drittdienstleister oder mit eng verbundenen IKT-Drittdienstleistern.“

„Für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, richten Finanzunternehmen Ausstiegsstrategien ein. …
Finanzunternehmen stellen sicher, dass sie aus vertraglichen Vereinbarungen ausscheiden können, ohne:
a) Unterbrechung ihrer Geschäftstätigkeit,
b) Einschränkung der Einhaltung regulatorischer Anforderungen,
c) Beeinträchtigung der Kontinuität und Qualität ihrer für Kunden erbrachten Dienstleistungen.“

Beispiel Finanzindustrie

Die europäische Aufsicht sieht die Konzentration von IKT-Dienstleistungen bei einigen Anbietern und die daraus folgende Abhängigkeit als so gravierend an, dass diese Anbieter selbst beaufsichtigt werden (müssen).

Liste sog. „kritischer IKT-Drittdienstleister“ i.S.v. Art. 31 ff. DORA

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

JOINT COMMITTEE OF THE EUROPEAN SUPERVISORY AUTHORITIES

In accordance with Article 31(9) of the Digital Operational Resilience Act, the list of designated critical ICT third-party service providers at Union level (in alphabetic order) is the following:

- Accenture plc
- Amazon web Services EMEA Sarl
- Bloomberg L.P.
- Capgemini SE
- Colt Technology Services
- Deutsche Telekom AG
- Equinix (EMEA) B.V.
- Fidelity National Information Services, Inc.
- Google Cloud EMEA Limited
- International Business Machine Corporation
- InterXion HeadQuarters B.V.
- Kyndryl Inc.
- LSEG Data and Risk Limited
- Microsoft Ireland Operations Limited
- NTT DATA Inc.
- Oracle Nederland B.V.
- Orange SA
- SAP SE
- Tata Consultancy Services Limited

Herausforderungen

bei der Beschaffung von souveräner IT

Leitplanken für rechtssichere Beschaffung souveräner IT

Definition der Souveränitätsgründe

GEOPOLITIK

- Politische / regulatorische Sanktionen
- Betrachtung von potenziellen Anfälligkeiten

REGULATORIK

- Sicherheits- und Compliance-Risiken
- Einschränkungen beim Datenzugriff / Datenstandort

TECHNOLOGIE

- Vendor lock-in
- Kostensteigerungen
- Verlust operativer Autonomie

Leitplanken für rechtssichere Beschaffung souveräner IT

Beschreibung des Zielbildes

- **Smarte Souveränität**: Intelligente Definition souveräner Lösungen – Nachhaltigkeit (Dauer, Kosten, Innovationsfähigkeit). Hieraus folgt regelmäßig Unterstützung hybrider Konzepte und schnellen Wandels, klare Trennung von Muss- und Soll-Anforderungen, sowie flexibel steuerbare „Schieberegler“.

- **Technische Anforderungen**: Ableitung der technischen Anforderungen aus den gesetzlichen und regulatorischen Vorgaben – harte Vorgaben (je nach Jurisdiktion u.U. (stark) divergierend) sowie darüber hinausgehende Anforderungen, die das Unternehmen an sich selbst stellt (weiche Vorgaben).

- **Etablierte Standards:** EU Cloud Sovereignty Framework, BSI Kriterien u.Ä. unterstützen Vergleichbarkeit und Kontrollpunkt.

SOVEREIGNITY STANDARD	INHALTLICHER FOKUS	RELEVENAZ FÜR SOVEREIGN IT
EU Cloud Sovereignty Framework	Rechtsbindung, Datenkontrolle, Zugriffsrisiken	Grundlage für EU-weite Anforderungen
BSI Souveränitätskriterien (2026)	Technische & operative Mindestanforderungen	Nationaler Maßstab für Behörden & Kritische Infrastruktur
C5-Kriterien	Cloud-spezifische Sicherheits- und Auditstandards	Nachweisbarkeit & Prüfpflichten
Sovereign Cloud Stack (SCS)	Offene Architektur, Föderation, Interoperabilität	Technische Grundlage für Gaia-X-konforme Cloud
…	…	…

Leitplanken für rechtssichere Beschaffung souveräner IT

Arten und Wege der Beschaffung

Direktbeschaffung

- Schnelles und kostengünstigeres Beschaffungsverfahren durch kürzere, informellere Entscheidungswege
- Freie Anbieterwahl, keine Festlegung auf kleinen Kreis von Ausschreibungsteilnehmern
- *Jedoch*: geringe Markttransparenz, tendenziell höhere laufende Kosten mangels Wettbewerb

Bei kleineren Beschaffungen oder hochstandardisierten Lösungen

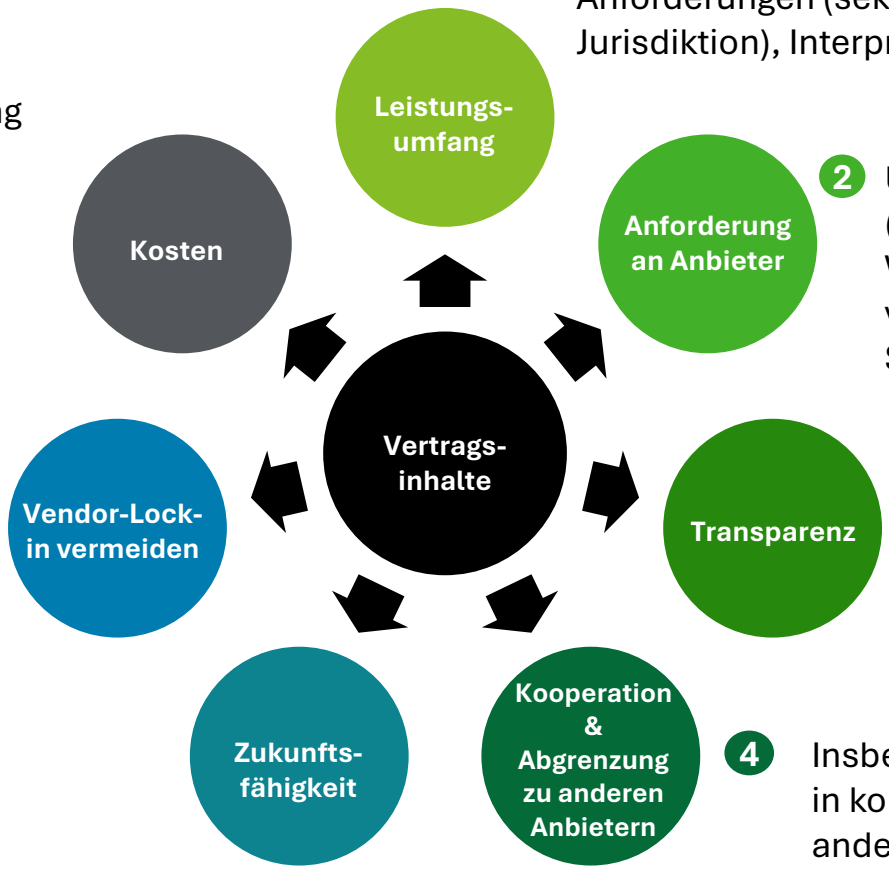
Ausschreibung

- Transparenz im Wettbewerb / Vergleichbarkeit von Anbietern erhöht die Chance, optimal passende Leistungen zu guten Konditionen zu beziehen
- Nachvollziehbare Entscheidungsprozesse & Compliance bei der Beauftragung
- *Jedoch*: je nach Ausgestaltung zeitintensivere Ausschreibungsverfahren (RfI, RfP, BAFO, Endverhandeln)

Bei großvolumigen Beschaffungen oder stark zugeschnittenen Lösungen

Leitplanken für rechtssichere Beschaffung souveräner IT

Besondere Anforderungen an die Vertragsinhalte



1 Insbesondere vom „Sonderlocken“ aufgrund spezifischer Anforderungen (sektor-/unternehmensspezifisch, je nach Jurisdiktion), Interpretation von Standards und internen Policies…

2 Unmittelbare und mittelbare Eigentumsverhältnisse (z.B. nur deutsche oder europäische Eigentümer), Wohnsitz & Nationalität der Mitarbeiter, vergleichbare Anforderungen bzgl. Subunternehmer, Hardwarelieferanten, …

3 Klare Audit-, Dokumentations- und Nachweispflichten, …

4 Insbesondere bei Hybrid-Modellen bzw. Einbindung in komplexe IT-Systeme einerseits enge Kooperation, andererseits klare Abgrenzung der Leistungspflichten notwendig, …

5 Sicherstellung Skalierbarkeit sowie Anpassungs-/Innovationsfähigkeit, zur fortlaufenden Möglichkeit der Anpassung der Lösung auf Bedarf, rechtliche Änderungen und Marktentwicklungen – ansonsten Investitionsrisiko, …

6 Klare Kündigungs- und Exit-Regelungen (ggf. Cloud Switching nach EU Data Act), Sicherstellung von Interoperabilität und offenen Standards für einfache Anbindung/Migration, ggf. Bereitstellung von Konfigurationen, Source Code o.Ä. laufend oder beim Exit, …

7 Je nach Skalierbarkeit oft deutlich höhere Betriebskosten, Gainsharing bei Innovation und Change, schwankende Hardwarepreise, …

Leitplanken für rechtssichere Beschaffung souveräner IT

Migration & Go-Live

Migration

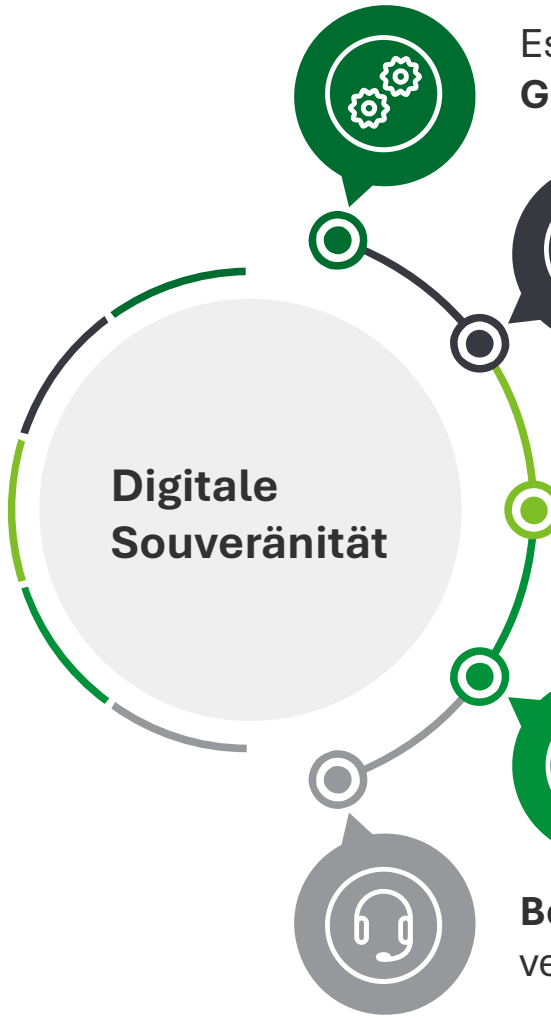
- Klare **Abnahmekriterien** im Hinblick auf **Migrationsleistungen**, insb. mit Blick auf **Souveränitätsanforderungen.**
- Gesteigerte Anforderungen an **Nachvollziehbarkeit** der einzelnen Migrationsschritte.
- Soweit möglich, Vermeidung von **Datentransfers** nach außerhalb der Zielregion.
- **Lösungsrechte (Kündigung, Rücktritt o.ä.)** bei Verstößen gegen vereinbarte Souveränitäts-anforderungen im Rahmen der Migration.

Go-Live

- Produktivbetrieb erst nach **Abnahme** auch aller souveränitätsspezifischen Kriterien.
- Für Übergangszeitraum kurz nach Go-Live („**Hypercare**“): ggf. Parallelbetrieb mit / Fallback auf Altsysteme erforderlich – auch insoweit muss Souveränität gewährleistet sein.
- **Löschzertifikate** bzgl. Daten auf Altsystemen (insb., soweit diese bislang auf Systemen außerhalb der neuen Zielregion lagen).
- Sicherstellung der Einhaltung der Souveränitätsanforderungen auch durch **Support-/Admin-Personal** sowie auf **Control-Plane-Ebene** (Identity Management, Auditing, Monitoring, Provisioning).

Zusammenfassung

Kernaussagen und Handlungsaufruf



Es gibt **drei Haupttreiber**, die einen Handlungsdruck bzgl. Digitaler Souveränität erzeugen - **Geopolitik, Regulatorik** und **Technologie.**

Es sollte **abgewogen werden** in welchen Bereichen des Unternehmens digitale Souveränität besonders wichtig ist und **mögliche Implikationen** bedacht werden.

Verschiedene souveräne Cloud Architekturen können genutzt werden, passend zu den definierten Souveränitäts-Zielen.

Regulierte Industrien sind bereits gezwungen, sich zur digitalen Souveränität zu positionieren – gleichzeitig entsteht hierdurch eine **best practice** in den Bereichen Risikoanalyse, Vertragsgestaltung und Ausstiegsstrategie.

Beschaffung von souveräner IT setzt einen **strukturierten Prozess** voraus – andernfalls drohen vermeidbare Kosten und Verfehlung der Ziele.

Deloitte Thought Leadership zu Digitaler Souveränität

Unsere aktuellen Insights zur digitalen Souveränität in wichtigen Branchen und Technologiebereichen

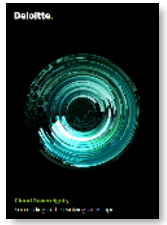
Overarching

Strategy, Sovereignty and Silicon
How Sovereign AI Capabilities Can Increase European Competitiveness

White Paper (2026)

Das digitale Deutschland im Jahr 2035
Technologische Souveränität, globale Innovationskraft und KI in vier Szenarien

White Paper (2025)



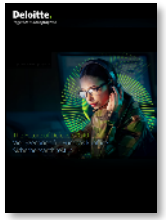
Cloud Sovereignty
Succeeding in the evolving landscape

White Paper (2025)

K-shaped globalization
How geopolitics is reshaping trade and investment corridors

White Paper (2026)

Sector



The Future of Defense 2040
Vier Szenarien für Europas künftige Sicherheitsarchitektur

White Paper (2026)

Akuter Handlungsbedarf im Gesundheitswesen
Erhöhung der Cyberresilienz von Krankenhäusern

White Paper (2025)

TMT Industry Briefing
Jeder Zweite sorgt sich um Deutschlands technologische Unabhängigkeit

Industry Briefing (2025)

Supply-Chain-Resilienz
Status quo und Ausblick für den Groß- und Außenhandel

White Paper (2025)

Ecosystem

Deloitte & AWS
Unlocking Europe's Competitive-ness with Sovereign Cloud
The Path to a trusted Digital Future

White Paper (2026)

Deloitte & Intel
Private Cloud Renaissance
The Power of Next-Generation Infrastructure

White Paper (2025)

Deloitte, ServiceNow & STACKIT
Compliant, Controlled, Confident:
The Next Era of Data and AI Sovereignty

White Paper (2025)

Deloitte & Oracle
Moderne Finanzsteuerung in Krankenhaus, Klinik & Praxis

White Paper (2025)

Q&A

Vielen Dank
für Ihre
Aufmerksamkeit

Deloitte Legal

Ihr Kontakt

Dr. Till Contzen
Co-Lead Digital Law
Rechtsanwalt | Partner (Deloitte Legal)

Tel.: +49 697 1918 8439
E-Mail: tcontzen@deloitte.de

Dr. Hannes Bracht
Banking & Finance
Rechtsanwalt | Partner (Deloitte Legal)

Tel.: +49 697 1918 8432
E-Mail: hbracht@deloitte.de

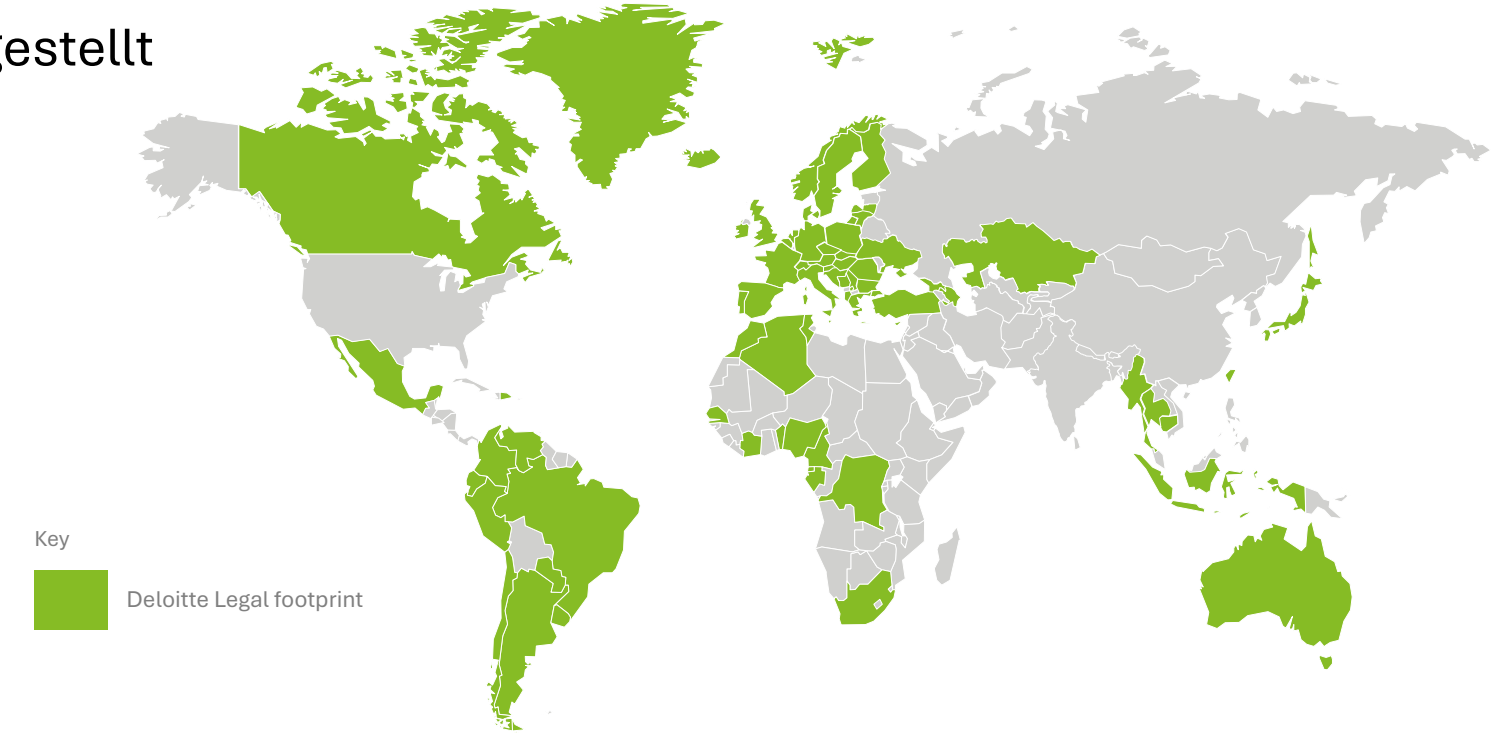
Daniel Lettmayer
Technology & Transformation
Senior Specialist Lead (Deloitte GmbH)

Tel.: +49 699 7137 1176
E-Mail: dlettmayer@deloitte.de

Deloitte Legal ist weltweit stark aufgestellt

Es kann sehr herausfordernd sein, eine Vielzahl von Rechtsberatern rund um die Welt zu koordinieren, ohne dabei einzelne Aspekte aus den Augen zu verlieren.

Als eine der weltweit führenden Rechtsberatungen unterstützt Deloitte Legal Sie bei der Bewältigung von Herausforderungen und der Verwirklichung Ihrer Vision; dabei ist Deloitte Legal Ihr zentraler Kontakt für Ihren weltweiten juristischen Beratungsbedarf.



Deloitte Legal practices

1. Albania
2. Algeria
3. Argentina
4. Australia
5. Austria
6. Azerbaijan
7. Belgium
8. Benin
9. Bosnia
10. Brazil
11. Bulgaria
12. Cambodia
13. Cameroon
14. Canada
15. Chile
16. Colombia
17. Costa Rica
18. Croatia
19. Cyprus
20. Czech Rep.
21. Dem Rep of Congo
22. Denmark
23. Dominican Republic
24. Ecuador
25. El Salvador
26. Equatorial Guinea
27. Finland
28. France
29. Gabon
30. Georgia
31. Germany
32. Greece
33. Guatemala
34. Honduras
35. Hong Kong SAR, China
36. Hungary
37. Iceland
38. Indonesia
39. Ireland
40. Italy
41. Ivory Coast
42. Japan
43. Kazakhstan
44. Kosovo
45. Latvia
46. Lithuania
47. Malta
48. Mexico
49. Montenegro
50. Morocco
51. Myanmar
52. Netherlands
53. Nicaragua
54. Nigeria
55. Norway
56. Paraguay
57. Peru
58. Poland
59. Portugal
60. Romania
61. Senegal
62. Serbia
63. Singapore
64. Slovakia
65. Slovenia
66. South Africa
67. Spain
68. Sweden
69. Switzerland
70. Taiwan
71. Thailand
72. Tunisia
73. Turkey
74. Ukraine
75. Uruguay
76. United Kingdom
77. Venezuela

Deloitte Legal