Digital Sovereignty

Hype or Paradigm Shift?

Deloitte Legal Webcast | June 17, 2026

Agenda & Introduction of the Speakers

Agenda

Introduction of the Speakers

Term Classification: Areas of Action in Digital Sovereignty

Legal Issues: The Case of the Financial Industry

Challenges in Procuring Sovereign IT

Summary

Q&A

Speakers

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

Phone: +49 697 1918 8439
Email: tcontzen@deloitte.de

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

Phone: +49 697 1918 8432
Email: hbracht@deloitte.de

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

Phone: +49 699 7137 1176
Email: dlettmayer@deloitte.de

Term Classification

Areas of Action in Digital Sovereignty

What drives organisations to act?

Regulatory and Technological Risks Take Center Stage in Discussions on Sovereignty – Geopolitics Is Often Perceived as Falling Outside the Sphere of Direct Influence

Focus on Sovereignty Triggers and Risks

GEOPOLITICS

- Political / Regulatory Sanctions
- Assessment of potential vulnerabilities

REGULATION

- Security and compliance risks
- Restrictions on data access / data location

TECHNOLOGY

- Vendor lock-in
- Cost Increases
- Loss of operational autonomy

What drives organisations to act?

Regulatory and Technological Risks Take Center Stage in Discussions on Sovereignty – Geopolitics Is Often Perceived as Falling Outside the Sphere of Direct Influence

Focus on Sovereignty Triggers and Risks

GEOPOLITICS

- Political/regulatory sanctions
- Assessment of potential vulnerabilities

REGULATION

- Security and compliance risks
- Restrictions on data access / data location

TECHNOLOGY

- Vendor lock-in
- Cost Increases
- Loss of operational autonomy

What drives organisations to act?

Regulatory and Technological Risks Take Center Stage in Discussions on Sovereignty – Geopolitics Is Often Perceived as Falling Outside the Sphere of Direct Influence

Focus on Sovereignty Triggers and Risks

GEOPOLITICS

- Political / Regulatory Sanctions
- Assessment of potential vulnerabilities

REGULATION

- Security and compliance risks
- Restrictions on data access / data location

TECHNOLOGY

- Vendor lock-in
- Cost Increases
- Loss of operational autonomy

The Decision-Maker's Sovereignty Dilemma

Decision-makers must align regulatory and geopolitical constraints with transformation and technology goals

Trade-offs

External Pressures

Sovereignty: Established ecosystems are being challenged by geopolitical events

Regulatory requirements: New, but as yet unclear, requirements for many industries—ensuring compliance with laws and guidelines.

Complexity of the technology stack: It's about more than just introducing a new cloud product—audit-proof, sovereign operational processes are required.

Sovereignty – Compliance

BALANCE

Value Creation & Innovation

Internal Priorities

Realising value from technology investments: Achieve ROI as quickly as possible for ERP, cloud, and AI initiatives to leverage efficiency potential.

Strategic Narratives & Market Alignment: Cloud decisions influence market perception and the dynamics within the ecosystem.

Operational Resilience & AI Readiness: Secure AI capabilities during the digital and sovereign transformation.

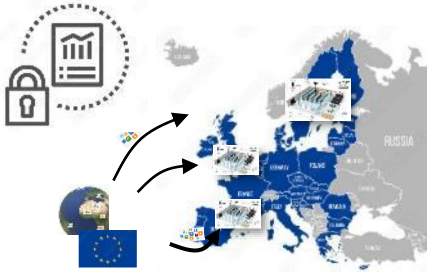
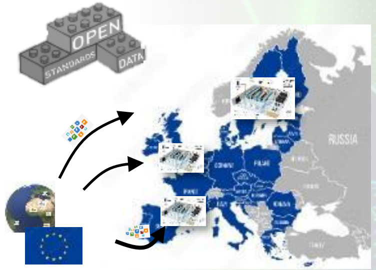
Sovereign cloud architectures

Sovereign cloud architectures can be divided into four archetypes that address different requirements. Identified risks are addressed through new service offerings from cloud providers.

Emerging sovereign cloud architectures

Cloud Deployment Models

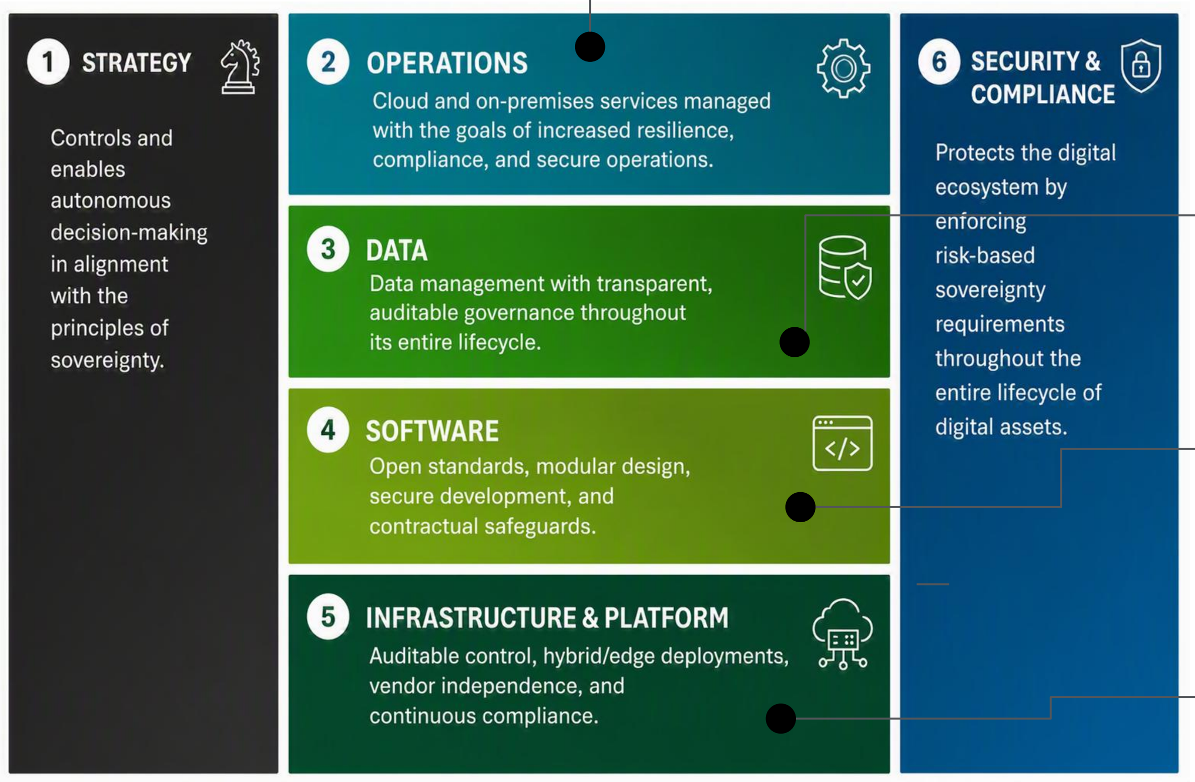
Private Cloud* | *Public Cloud* | *Hybrid Cloud* | *Community Cloud

Centralised Management		***Decentralised Management***	
			
1 U.S. hyperscalers with EU-compliant offerings	2 EU-native cloud Service Provider	3 Proprietary technology on EU-owned infrastructure	4 Open-source solutions on EU-owned infrastructure

Approach to Digital Sovereignty

Our experts from various fields—ranging from strategy and consulting to managed services—have developed a holistic framework that guides organizations through the immense complexity of this topic

Deloitte's Digital Sovereignty Framework



- Operational framework, data residency controls, access policies
- disaster recovery strategies, failover readiness, continuity planning
- Monitoring, SLA enforcement, incident response capabilities

- Approach and fundamentals for data lifecycle management
- Data sensitivity, encryption, regulatory compliance
- Policies for data access, data sharing, and interoperability

- Software IP, contractual restrictions, reversibility options
- Exit strategies, interoperability, cloud-native architectures
- Practices for code audits, open-source usage, DevSecOps

- Infrastructure design, workload placement, platform selection
- Integrating workload portability and sovereign platforms
- Sovereignty-compliant computing, storage, and network configurations

Tool for accelerated implementation

To address digital sovereignty, we use a suite of AI agents to define specific requirements and a roadmap for implementation

Deloitte’s Digital Sovereignty Navigator – SONA

Assessing company-specific risks related to sovereignty using our Digital Sovereignty Framework

- Understand **the regulatory drivers, cloud architectures**, **and** vendor **solutions** that shape your industry.
- Identify **critical workloads, risk scenarios,** and the foundation for your company’s sovereignty.
- Discuss **compliance requirements, security, and economic considerations**—with actionable migration paths.

Supported by:

SONA

Deloitte’s AI-based Sovereignty Navigator tool

Use Cases in a Regulated Environment

Sovereign Cloud Infrastructure for SANA Clinic with STACKIT*

Sana is a leading German healthcare provider with more than 41,000 employees and 46 hospitals. Sana is undergoing a digital transformation driven by requirements for electronic health records.

Objective: To establish an additional sovereign cloud platform for critical services as part of an existing hybrid and multicloud strategy, based on STACKIT

Data sovereignty: Aspects of the GDPR, BSI-C5, and the Hospital Future Act, including the requirement to keep patient data within the EU.

A central cloud platform is required to offer future IT services across locations in a sovereign manner.

Setting up a scalable environment (Kubernetes containers) for the rollout of additional IT services.

Establishing a partnership: Partnership with STACKIT and Deloitte as consulting partners for design and implementation.

In-house skill development to enable the independent, long-term operation of the new, sovereign platform.

* German cloud service provider owned by the Schwarz Gruppe

Sovereign Cloud Infrastructure at a European Public Financial Institution Using an EU Cloud Provider

A major European public financial institution has reassessed its cloud risks for critical services in the U.S. cloud in light of geopolitical changes, resulting in a revised cloud strategy to strengthen digital sovereignty and mitigate dependency risks for critical services.

Key Challenges:

- The changed geopolitical landscape in 2025 led to increased risk exposure in the cloud sector, particularly due to dependence on U.S.-based hyperscalers
- Increased risks regarding sovereignty (availability) and vendor lock-in affecting business-critical services in the U.S. cloud
- The need to identify appropriate risk mitigation measures
- Evaluation of alternative hosting and cloud service models for risk mitigation
- Goal: A clear roadmap for risk mitigation and the definition of an implementation plan

Result:

- Identification of affected critical services and revision of the cloud strategy, with a focus on digital sovereignty and risk mitigation
- Implementation of a “Sovereign Cloud Landing Zone” with an EU-based cloud provider, enabling the migration of selected critical services and reducing dependency risks
- Reduced risks associated with dependence on U.S. providers and improved resilience for cloud-based critical services

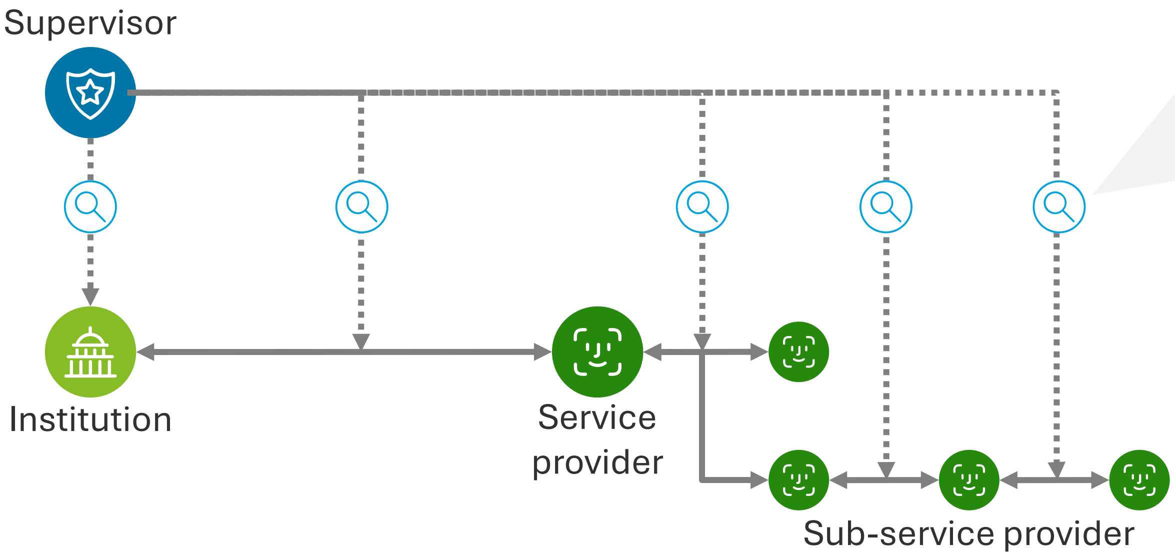
Legal Issues

The Case of the Financial Industry

Example: The Financial Industry

Given the high level of regulation and the sector's macroeconomic significance, the discussion of digital sovereignty in the financial industry is of particular importance.

Basic Principle of Supervision in the Digital Environment



Key Regulatory Mechanisms in the Banking Sector

- German Banking Act ("KWG")
- Digital Operational Resilience Act ("DORA")
- Guidelines on Outsourcing by the European Banking Authority ("EBA")
- Minimum Requirements for Risk Management ("MaRisk") by the Federal Financial Supervisory Authority ("BaFin")
- BaFin Supervisory Notice on Outsourcing to Cloud Providers
- Guidance on Outsourcing Cloud Services to Cloud Providers by the European Central Bank ("ECB")

Example: The Financial Industry

“Digital sovereignty” itself is not a term used in (banking) regulatory law, but a number of requirements contribute to digital sovereignty and provide a basis for best practices even in the unregulated sector.

Exemplary requirements for contractual arrangements, risk analysis, and exit

“In the event of outsourcing, the institution remains responsible for compliance with the legal provisions to which it is subject.”

“With regard to sub-outsourcing, the outsourcing agreement should, where possible, include provisions requiring the consent of the outsourcing institution or specify concrete conditions under which sub-outsourcing of individual work and process steps is permitted.”

“The outsourcing agreement should allow for the transfer of the outsourced function to another service provider or its reintegration into the institution or payment institution. To this end, the written outsourcing agreement should include the following provisions: ...”

“As part of the risk analysis, the following should generally be considered: ... concentration risks ... access to data by other jurisdictions ...”

“When identifying and assessing the ... risks mentioned above, financial institutions shall take into account ...:
a) Contracts with a third-party ICT service provider that cannot be readily replaced; or
b) multiple contractual agreements ... with the same third-party ICT service provider or with closely related third-party ICT service providers.”

“For ICT services that support critical or important functions, financial firms shall establish exit strategies.
...
Financial firms shall ensure that they can terminate contractual arrangements without:
a) disrupting their business operations,
b) compromising compliance with regulatory requirements,
c) compromising the continuity and quality of the services they provide to customers.”

Example: The Financial Industry

The European regulator considers the concentration of ICT services among a few providers and the resulting dependence to be so serious that these providers themselves (must) be subject to oversight.

List of "critical third-party ICT service providers" within the meaning of Art. 31 et seq. of DORA

European Banking Authority

European Insurance and Occupational Pensions Authority

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

Challenges

in Procuring Sovereign IT

Guidelines for Legally Sound Procurement of Sovereign IT

Definition of the Grounds for Sovereignty

GEOPOLITICS

- Political / Regulatory Sanctions
- Assessment of Potential Vulnerabilities

REGULATION

- Security and Compliance Risks
- Restrictions on Data Access / Data Location

TECHNOLOGY

- Vendor lock-in
- Cost Increases
- Loss of Operational Autonomy

Guidelines for Legally Sound Procurement of Sovereign IT

Description of the Target State

- **Smart Sovereignty**: Intelligent definition of sovereign solutions—sustainability (duration, costs, capacity for innovation). This typically entails support for hybrid concepts and rapid change, a clear distinction between mandatory and recommended requirements, as well as flexibly adjustable "sliders."

- **Technical Requirements**: Derivation of technical requirements from legal and regulatory mandates—hard requirements (which may vary (significantly) depending on jurisdiction) as well as additional requirements that the company sets for itself (soft requirements).

- **Established Standards:** The EU Cloud Sovereignty Framework, BSI criteria, and similar standards support comparability and serve as checkpoints.

SOVEREIGNTY STANDARD	CONTENT FOCUS	RELEVANCE FOR SOVEREIGN IT
EU Cloud Sovereignty Framework	Legal Compliance, Data Control, Access Risks	Foundation for EU-wide requirements
BSI Sovereignty Criteria (2026)	Minimum Technical & Operational Requirements	National standard for government agencies & critical infrastructure
C5 Criteria	Cloud-specific security and audit standards	Verifiability & Audit Requirements
Sovereign Cloud Stack (SCS)	Open Architecture, Federation, Interoperability	Technical foundation for a Gaia-X-compliant cloud
...	...	...

Guidelines for Legally Sound Procurement of Sovereign IT

Types and Methods of Procurement

Direct Procurement

- Faster and more cost-effective procurement process through shorter, more informal decision-making channels
- Free choice of suppliers; no restriction to a small group of bidders
- *However*: low market transparency, with a tendency toward higher ongoing costs due to a lack of competition

For smaller procurements or highly standardised solutions

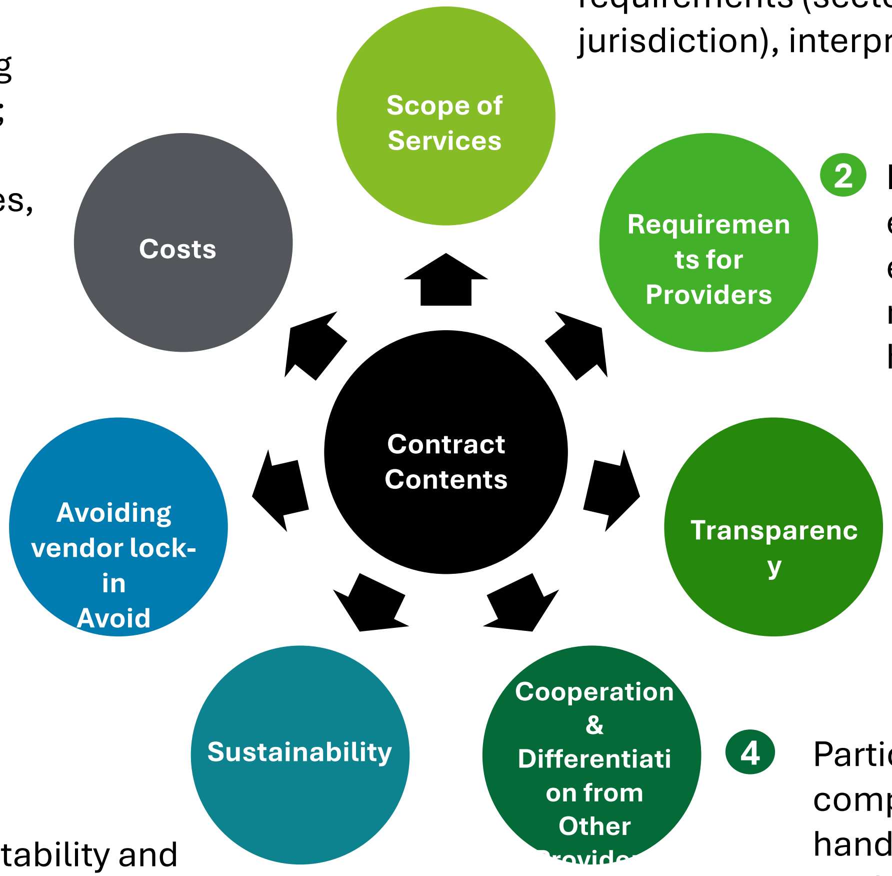
Request for Proposals

- Transparency in competition and the ability to compare suppliers increase the likelihood of obtaining the best-suited services on favorable terms
- Transparent decision-making processes and compliance in the awarding of contracts
- *However*: Depending on the structure, more time-consuming bidding processes (RfI, RfP, BAFO, final negotiations)

For high-volume procurements or highly customised solutions

Guidelines for Legally Sound Procurement of Sovereign IT

Special Requirements for Contract Terms



1. In particular, "special considerations" arising from specific requirements (sector- or company-specific, depending on jurisdiction), interpretation of standards, and internal policies...

2. Direct and indirect ownership structures (e.g. exclusively German or European owners), employees' residence and nationality, comparable requirements regarding subcontractors and hardware suppliers, ...

3. Clear audit, documentation, and verification requirements, ...

4. Particularly with hybrid models or integration into complex IT systems, close cooperation on the one hand and a clear delineation of service obligations on the other are necessary, ...

5. Ensuring scalability as well as adaptability and innovation capacity, to allow for the ongoing adaptation of the solution as needed, in response to legal changes and market developments—otherwise, there is an investment risk, ...

6. Clear termination and exit provisions (including cloud switching under the EU Data Act, if applicable), ensuring interoperability and open standards for easy integration/migration, and, if necessary, providing configurations, source code, or similar on an ongoing basis or upon exit, ...

7. Depending on scalability, operating costs are often significantly higher; gain-sharing for innovation and change; fluctuating hardware prices, ...

Guidelines for Legally Compliant Procurement of Sovereign IT

Migration & Go-Live

Migration

Clear **acceptance criteria** for **migration services**, particularly with regard to **sovereignty requirements.**

Increased requirements for **traceability** of individual migration steps.

Avoid **data transfers** outside the target region to the extent possible.

Remedies (termination, withdrawal, etc.) in the event of violations of agreed-upon sovereignty requirements during the migration.

Go-Live

Production operation only after **acceptance** of all sovereignty-specific criteria.

For the transition period shortly after go-live ("hypercare"): parallel operation with or fallback to legacy systems may be required—sovereignty must also be guaranteed in this regard.

Deletation certificates: regarding data on legacy systems (especially if this data was previously stored on systems outside the new target region).

Ensuring compliance with sovereignty requirements, including by **support and administrative staff,** as well as at **the control plane level** (identity management, auditing, monitoring, provisioning).

Summary

Key Messages and Call to Action

Digital Sovereignty

There are **three main drivers** creating pressure to act on digital sovereignty: **geopolitics, regulation,** and **technology.**

It is **important to assess** in which areas of the company digital sovereignty is particularly important and to consider **the potential implications**.

Various sovereign cloud architectures can be utilized, tailored to the defined sovereignty goals.

Regulated industries are already being forced to take a stance on digital sovereignty—at the same time, this is giving rise to **best practices** in the areas of risk analysis, contract drafting, and exit strategies.

Procuring sovereign IT requires a **structured process**—otherwise, there is a risk of incurring avoidable costs and failing to meet objectives.

Deloitte Thought Leadership on Digital Sovereignty

Our latest insights on digital sovereignty in key industries and technology sectors

Overarching

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

White Paper (2026)

Digital Germany in 2035
Technological Sovereignty, Global Innovation, and AI in Four Scenarios

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
Four Scenarios for Europe's Future Security Architecture

White Paper (2026)

Urgent Need for Action in the Healthcare
Increasing Cyber Resilience in hospitals

White Paper (2025)

TMT Industry Briefing
One in two people is concerned about Germany's technological independence

Industry Briefing (2025)

Supply Chain Resilience
Current Status and Outlook for Wholesale and Foreign Trade

White Paper (2025)

Ecosystem

Deloitte & AWS
Unlocking Europe's Competitiveness with Sovereign Cloud
The Path to a Trusted Digital Future

White Paper (2026)

Deloitte & Intel
The 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
Modern Financial Management in Hospitals, Clinics, and Medical Practices

White Paper (2025)

Q&A

Thank you very much

for your attention

Deloitte Legal

Your Contact

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

Phone: +49 697 1918 8439
Email: tcontzen@deloitte.de

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

Phone: +49 697 1918 8432
Email: hbracht@deloitte.de

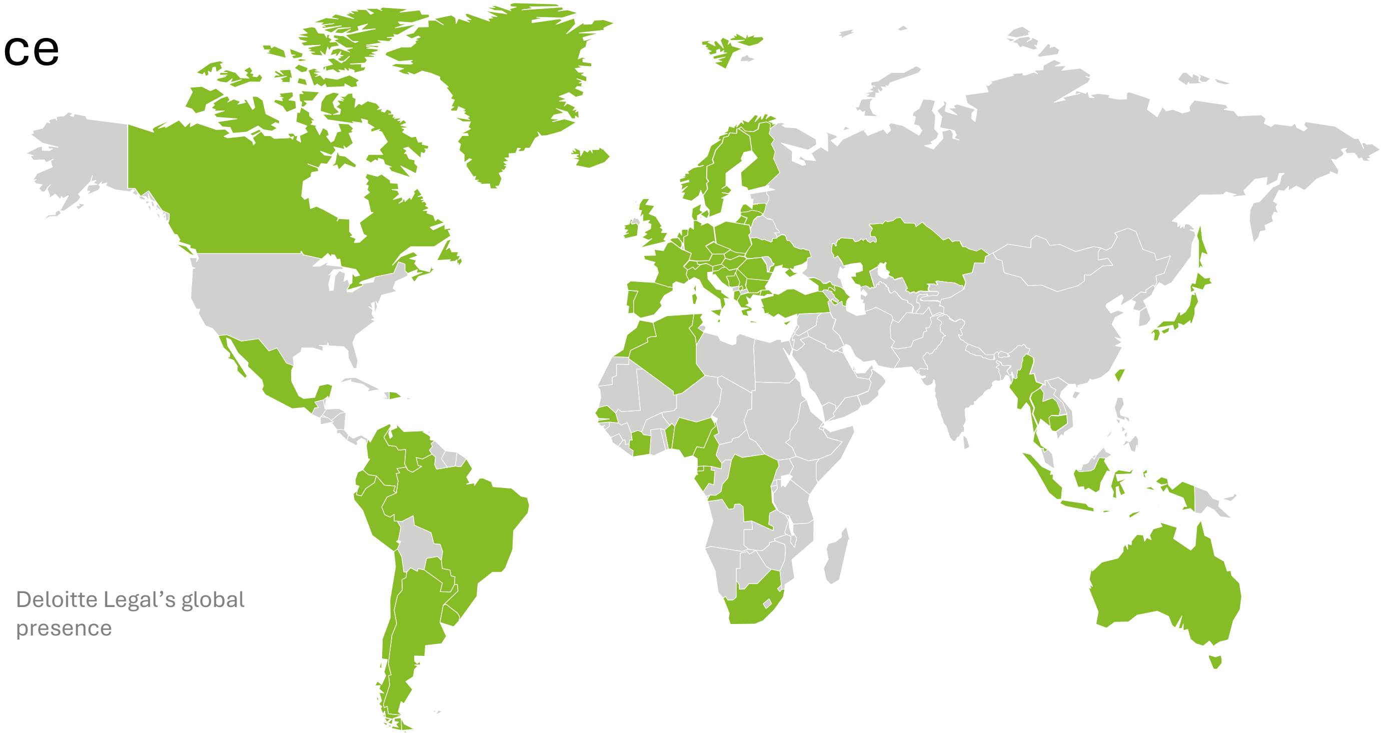
Daniel Lettmayer
Technology & Transformation
Senior Specialist Lead (Deloitte GmbH)

Phone: +49 699 7137 1176
Email: dlettmayer@deloitte.de

Deloitte Legal has a strong global presence

It can be very challenging to coordinate a large number of legal advisors around the world without losing sight of individual details.

As one of the world's leading law firms, Deloitte Legal helps you overcome challenges and realize your vision; Deloitte Legal serves as your single point of contact for all your global legal needs.



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 Republic
21. Democratic Republic of the 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