J.KELLER - CONSULTING
Business Resilience & Compliance
Enterprise Security & Risk Management

Resilienz & Datenhoheit: Sicher in die digitale Zukunft

In einer zunehmend vernetzten Welt wird die Kontrolle über Daten und IT-Systeme zur strategischen Notwendigkeit. Diese Präsentation beleuchtet die zentralen Säulen digitaler Souveränität in Deutschland und Europa.

Warum digitale Souveränität jetzt entscheidend ist!

Deutschland positioniert sich als Voreiter für Europas digitale Souveränität und Cyber-Resilienz. Die strategische Ausrichtung zielt auf die Unabhängigkeit von nicht-europäischen Anbietern und den Schutz kritischer Infrastrukturen ab.

Die Bundesregierung investiert Milliarden in Cyberabwehr und den Aufbau digitaler Infrastruktur. Diese Investitionen sind nicht nur eine Reaktion auf geopolitische Spannungen, sondern eine proaktive Maßnahme zur Sicherung der technologischen Handlungsfähigkeit.

Laut Pexip (2025) wird Deutschland zum Schlüsselakteur in der Gestaltung europäischer Standards für Datensicherheit und digitale Unabhängigkeit. Die Zeit zu handeln ist jetzt.

GRC – Governance, Risk & Compliance im Datenschutz

Datenschutz bildet den Kern der Datenhoheit. Die DSGVO hat sich als globaler Standard etabliert und prägt weltweit die Gestaltung von Datenschutzgesetzen.

DSGVO-Compliance

Strenge Anforderungen an Datenverarbeitung, Auskunftsrechte und Dokumentation als Grundlage digitaler Souveränität

Neue Regulierungen

DORA, NIS2 und CRA erweitern die Pflichten für Unternehmen und Behörden erheblich

NIS2 in der Praxis

Kritische Infrastrukturen müssen strenge Meldepflichten bei Sicherheitsvorfällen einhalten

Die erfolgreiche Umsetzung dieser Vorgaben erfordert eine ganzheitliche GRC-Strategie, die technische, organisatorische und rechtliche Aspekte vereint.

Information Security & Cloud Security (C5-Standard)

C5-Zertifizierung

Der Cloud Computing Compliance Criteria Catalogue (C5) des BSI ist zum Maßstab für Cloud-Sicherheit in Deutschland geworden. Er definiert Mindestanforderungen an sichere Cloud-Dienste.

Das AWS Nitro System demonstriert technische Ansätze zur Isolation: Hardware-basierte Sicherheit verhindert Datenzugriff durch Betreiber und schafft Vertrauen in Cloud-Infrastrukturen.

Europäische Herausforderung

Die Debatte „Made in Europe" versus US-Hyperscaler bleibt aktuell. Der US CLOUD Act ermöglicht Datenzugriff durch US-Behörden – ein Konflikt mit europäischen Datenschutzanforderungen.

Deutsche und europäische Cloud-Anbieter gewinnen an Bedeutung, wenn Datenhoheit und rechtliche Kontrolle Priorität haben.

Data Governance: Kontrolle und Verantwortung über Daten

01

Data Sovereignty vs. Data Residency

Data Residency beschreibt den physischen Speicherort von Daten. Data Sovereignty geht weiter: Sie umfasst die rechtliche Kontrolle über Daten, unabhängig vom Standort. Für EU-Unternehmen bedeutet dies, dass Daten europäischem Recht unterliegen müssen.

02

Gaia-X Initiative

Gaia-X ist die europäische Antwort auf amerikanische und asiatische Cloud-Dominanz. Die Initiative schafft eine föderierte, interoperable Dateninfrastruktur mit europäischen Werten: Transparenz, Portabilität und Souveränität.

03

Praktische Umsetzung

Deutsche Unternehmen setzen zunehmend auf lokale Cloud- und Speicherlösungen. Hybride Architekturen ermöglichen Flexibilität bei gleichzeitiger Wahrung der Datenhoheit für sensible Informationen.

AI Governance & Compliance: Regeln für Künstliche Intelligenz

Mit dem EU AI Act tritt 2025 der weltweit erste umfassende Rechtsrahmen für KI-Systeme in Kraft. Er klassifiziert KI-Anwendungen nach Risikoklassen und definiert entsprechende Anforderungen.

Transparenz & Dokumentation

KI-Systeme müssen nachvollziehbar sein. Dokumentationspflichten umfassen Trainingsdaten, Algorithmen und Entscheidungslogiken.

Risikomanagement

Hochrisiko-KI erfordert strenge Prüfverfahren, kontinuierliches Monitoring und menschliche Aufsicht bei kritischen Entscheidungen.

Ethische Nutzung

Diskriminierungsverbote, Fairness-Anforderungen und Schutz der Grundrechte stehen im Zentrum ethischer KI-Governance.

AI-Leitlinien als Wettbewerbsvorteil: Unternehmen, die frühzeitig interne AI-Governance etablieren, minimieren rechtliche Risiken und schaffen Vertrauen bei Kunden und Partnern. Compliance wird zum strategischen Differenzierungsmerkmal.

Resilienz: Business Continuity & Disaster Recovery

Resilienz schützt Organisationen vor Cyberangriffen, technischen Ausfällen und geopolitischen Risiken. Eine resiliente IT-Infrastruktur ist keine Option mehr – sie ist überlebenswichtig.

Modularisierung statt Monolithen

Flexible, modulare IT-Architekturen erhöhen die Ausfallsicherheit dramatisch. Microservices und Cloud-native Ansätze ermöglichen es, einzelne Komponenten zu isolieren und schnell wiederherzustellen.

- Redundante Systeme an geografisch verteilten Standorten
- Automatisierte Failover-Mechanismen
- Regelmäßige Disaster-Recovery-Tests
- Incident-Response-Pläne mit klaren Verantwortlichkeiten

> **Praxisbeispiel:** Die deutsche Bundeswehr und Betreiber kritischer Infrastrukturen investieren massiv in robuste IT-Systeme. Ziel ist die Aufrechterhaltung der Handlungsfähigkeit selbst unter Angriffsbedingungen.

Regulatorik & gesetzliche Vorgaben im Überblick

Die regulatorische Landschaft entwickelt sich rasant. Drei zentrale Verordnungen prägen aktuell die Compliance-Anforderungen:

DORA

Digital Operational Resilience Act

EU-weite Anforderungen speziell für den Finanzsektor. DORA verpflichtet Finanzinstitute zu robustem IKT-Risikomanagement, Incident-Reporting und strengen Tests der operativen Widerstandsfähigkeit.

- Gilt ab Januar 2025
- Umfasst Banken, Versicherungen, Investmentfirmen
- Quartalsweise Sicherheitstests verpflichtend

NIS2

Network and Information Security Directive 2

Erweiterte Sicherheits- und Meldepflichten für kritische Sektoren. NIS2 betrifft erheblich mehr Unternehmen als die Vorgängerversion und schärft Sanktionen bei Nichteinhaltung.

- 18 kritische Sektoren abgedeckt
- 24-Stunden-Meldepflicht bei Vorfällen
- Persönliche Haftung für Geschäftsführung

CRA

Cyber Resilience Act

Neue Produktsicherheitsanforderungen für digitale Produkte und IoT-Geräte. Der CRA etabliert verbindliche Cybersecurity-Standards über den gesamten Produktlebenszyklus.

- CE-Kennzeichnung mit Cybersecurity-Anforderungen
- Verpflichtung zu Security-Updates
- Meldepflicht für aktiv ausgenutzten Schwachstellen

Zukunftsausblick: Technologische Souveränität und europäische Zusammenarbeit

Das FITS2030-Programm (Forschung, Innovation und Technologische Souveränität) definiert Deutschlands strategische Ausrichtung für die kommenden Jahre. Es kombiniert Forschungsförderung mit gezieltem Infrastrukturausbau.

Rechenzentren
Aufbau energieeffizienter, souveräner Rechenzentrumskapazitäten in Deutschland und Europa

KI-Entwicklung
Investitionen in europäische KI-Forschung und -Anwendungen, um Abhängigkeiten zu reduzieren

Quantentechnologie
Pionierarbeit im Quantencomputing als Grundlage zukünftiger technologischer Überlegenheit

Cybersecurity
Ausbau von Cybersecurity-Kompetenzen und -Infrastrukturen zum Schutz digitaler Souveränität

> **Vision 2030:** Europa als digital souveräne, resiliente und vernetzte Gemeinschaft – technologisch unabhängig, wirtschaftlich wettbewerbsfähig und werteorientiert in der Gestaltung der digitalen Zukunft.

Fazit: Resilienz & Datenhoheit als Fundament der digitalen Souveränität

Schutz von Wirtschaft, Gesellschaft und Demokratie

Digitale Souveränität ist keine technische Spielerei, sondern essenziell für den Schutz unserer demokratischen Werte und wirtschaftlichen Prosperität.

Ganzheitliche Governance

Starke Sicherheitsstandards, regulatorische Klarheit und proaktives Risikomanagement bilden das Fundament digitaler Handlungsfähigkeit.

Handeln Sie jetzt

Investitionen in Resilienz, Datenkontrolle und technologische Unabhängigkeit sind nicht optional – sie sichern die Zukunftsfähigkeit Ihres Unternehmens und unseres Kontinents.

Die digitale Transformation erfordert mehr als technische Lösungen. Sie verlangt nach einer strategischen Vision, die Sicherheit, Innovation und europäische Werte vereint. Die Werkzeuge stehen bereit – nutzen wir sie gemeinsam für eine souveräne digitale Zukunft.

Impressum

J.KELLER - CONSULTING
Business Resilience & Compliance
Enterprise Security & Risk Management

Herausgeber & verantwortlich für den Inhalt:

J. Keller-Consulting
Inhaber: Jürgen Keller
Fichtenstr. 13, D-85659 Forstern
Kontakt: Telefon: +49 8124 523481
E-Mail: juergen.keller@jkeller-consulting.de
Website: www.jkeller-consulting.de