CYBERSECURITY & RESILIENCE

CII WHITE PAPER

# Europäische Datensouveränität und digitale Prozess-verantwortung

Prof. Dr. Dennis-Kenji Kipker

CYBER|INTELLIGENCE
.Institute

# Inhalt

# 1. Einleitung

Die Sicherstellung von Datensouveränität entwickelt sich zu einer zentralen Voraussetzung für die digitale Handlungsfähigkeit europäischer Organisationen. Unter Datensouveränität wird kontextbezogen die Fähigkeit europäischer Unternehmen und Organisationen verstanden, Daten unabhängig, sicher und unter Beachtung rechtlicher Vorgaben zu erzeugen, zu verarbeiten, zu speichern und zu teilen[1]. Sie umfasst sowohl die technische Kontrolle über Datenflüsse als auch die rechtliche und organisatorische Verantwortung für deren Nutzung.

Die Abhängigkeit europäischer Staaten und Institutionen von außereuropäischen Technologieanbietern verdeutlicht insbesondere die **geopolitische Dimension** dieser Herausforderung. Infrastruktur, Kommunikationssysteme und kritische Verwaltungsprozesse basieren in Teilen auf Plattformen und Diensten, die außerhalb des europäischen Rechtsraums entwickelt und betrieben werden. Damit verbunden sind Fragen nach Transparenz, Kontrolle und Durchsetzbarkeit europäischer Standards.[2]

> **Geopolitische Konflikte, hybride Bedrohungen und wirtschaftliche Rivalitäten erzeugen einen wachsenden Druck auf Regierungen, Behörden und Unternehmen, ihre digitale Souveränität zu stärken.**

Zunehmend geraten zudem nationale Infrastrukturen in das Zentrum internationaler Spannungen. Geopolitische Konflikte, hybride Bedrohungen und wirtschaftliche Rivalitäten erzeugen einen wachsenden Druck auf Regierungen, Behörden und Unternehmen, ihre digitale Souveränität zu stärken. Dies zeigt sich aktuell auch in einer deutlichen Zunahme leistungsfähiger **DDoS-Angriffe** auf Betreiber kritischer Infrastrukturen in Deutschland, insbesondere im Energie-, Verwaltungs- und Gesundheitssektor.[3] Die Angriffe reichen von großvolumigen Backbone-Attacken bis hin zu gezielten Applikationsangriffen, die bestehende Schutzmechanismen umgehen und essenzielle Dienste gezielt lahmlegen.

Datensouveränität wird damit nicht allein zu einer technischen oder organisatorischen Anforderung, sondern zu einem **strategischen Faktor** für Resilienz, Rechtssicherheit und Wettbewerbsfähigkeit. Vor diesem Hintergrund ist die Entwicklung rechtskonformer, verschlüsselter und nachvollziehbarer Prozesse kein optionales Ziel mehr, sondern eine strukturelle Notwendigkeit, um die Vertrauenswürdigkeit von Technologie in unsicheren Zeiten technisch belastbar beurteilen zu können. Dieser zunehmende Trend hin zu digitaler Resilienz ist jedoch immer weniger optionaler Zusatz, sondern rechtlich verpflichtende Vorgabe insbesondere in den hochregulierten Branchen, aber darüber hinaus ebenso im Sinne einer allgemeinen wirtschaftlichen Gewährleistungsverantwortung. Organisationen im Gesundheitswesen, in der öffentlichen Verwaltung und in anderen regulierten Branchen stehen deshalb vor der Aufgabe, ihre digitalen Strukturen so auszurichten, dass sie künftigen Vorgaben standhalten und gleichzeitig nachhaltige Souveränität gewährleisten – dies kann nur durch frühzeitiges, planvolles und strategisches Handeln gelingen.

1 Vgl. Beise, „Datensouveränität und Datentreuhand“, RDi 2021, 597 (598) oder Denga, „Digitale Souveränität durch Datenprivatrecht?“, GRUR 2022, 1113 (1113 ff.).

2 Heckmann/Paschke, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl. 2022, § 121 Digitalisierung und Grundrechte, Rn. 59.

3 https://www.security-insider.de/zunahme-ddos-attacken-1hj-2025-a-da7e15ad0ca8bf947f5a5d8d98110f88/, zuletzt abgerufen am: 26.09.2025.

# 2. Überblick regulatorischer Rahmenbedingungen zur europäischen Datensouveränität

Die europäische Regulierung für den digitalen Raum entwickelt sich in hoher Geschwindigkeit und im internationalen Vergleich federführend über unterschiedlichste Technologiebereiche hinweg. In den vergangenen Jahren sind verschiedene regulatorische Rahmenbedingungen neu in Kraft getreten bzw. wirksam geworden, die die Frage europäischer Datensouveränität entscheidend mitbestimmen. Diese **Gesetzeswerke** werden perspektivisch tiefgreifende Auswirkungen auf die Gestaltung von Prozessen im Gesundheitswesen, in der öffentlichen Verwaltung und anderen regulierten Branchen haben. Die neuen IT-regulatorischen Vorgaben setzen dabei nicht nur kleine Impulse, sondern verändern die strategischen Grundlagen digitaler Souveränität in Europa jetzt und in Zukunft nachhaltig. Im Folgenden werden einige der wichtigsten dieser Rahmenbedingungen und ihre Auswirkungen vorgestellt:

## 2.1 EU Data Act

Der **EU Data Act** bildet das Kernstück der europäischen Datenstrategie.[4] Er schafft Regeln für den Zugang zu und die Weitergabe von Daten zwischen Unternehmen, Organisationen und Behörden. Für Akteure in kritischen Sektoren bedeutet dies, dass Datennutzung und -austausch künftig in klaren rechtlichen Bahnen erfolgen müssen. Insbesondere gilt:

- **Verpflichtender Zugang** zu Daten für Nutzer:innen
- **Vermeidung einseitiger Abhängigkeiten** von Technologieanbietern durch Vorgaben zur Interoperabilität
- **Pflicht zur Vertragstransparenz**, insoweit also neue Anforderungen an die Vertragsgestaltung[5]

Für das Gesundheitswesen eröffnet der Data Act mit seinem Rahmenwerk zum Datenzugang durchaus neue Chancen zur besseren Nutzung medizinischer Daten, stellt aber zugleich hohe Anforderungen an Verschlüsselung, Zugriffskontrolle und Nachvollziehbarkeit auf. Ähnliche Vorgaben enthält das nationale Gesundheitsdatennutzungsgesetz (GDNG), indem insbesondere Ausnahmen vom datenschutzrechtlichen Zweckbindungsgrundsatz normiert werden – bei gleichzeitig steigenden Vorgaben an die technische und organisatorische Datensicherheit. Wo somit einerseits Privilegien definiert werden, schlagen diese sich andererseits in verstärkten Schutzanforderungen sensibler Daten nieder.

## 2.2 EU NIS2-Richtlinie

Die **EU NIS2-Richtlinie** zur Cybersicherheit ist im Dezember 2022 in Kraft getreten und war bis zum Oktober 2024 in das mitgliedstaatliche Recht umzusetzen. In Deutschland ist die Umsetzung verspätet, zurzeit wird davon ausgegangen, dass die Umsetzung zu Ende 2025/Anfang 2026 erfolgt. Die NIS2-Richtlinie verpflichtet Unternehmen und Institutionen in mehr als 18 kritischen Sektoren, darunter Gesundheitsversorgung, öffentliche Verwaltung, Energie und Transport, zu umfassenden Maßnahmen in der Cybersicherheit.[6] Kernelemente sind:

- **Risikomanagement** und Einführung technischer wie organisatorischer Sicherheitsstandards unter umfassender Berücksichtigung der Resilienz der digitalen Lieferkette
- **Meldepflichten** für Sicherheitsvorfälle mit strengen Zeitvorgaben
- **Haftung und Sanktionen** bei Nichterfüllung, einschließlich persönlicher Verantwortung der Geschäftsführung

4 Siehe beispielsweise Metzger, „Datenschutz oder Datenzugang? Neuausrichtung des europäi-schen Datenrechts nach dem Data Act“, NJW 2025, 2729 für einen Überblick.

5 Pommerening/Nickel, Wechsel zwischen Datenverarbeitungsdiensten nach dem Data Act, RDi 2024, 289 (289 ff.)

6 https://cyberintelligence.institute/news-media/nis-2-referentenentwurf-updates-analysen-hintergruende, zuletzt abgerufen am: 26.09.2025.

Für betroffene Institutionen und Unternehmen bedeutet dies, dass sie ihre Prozesse so strukturieren müssen, dass sie jederzeit dahingehend transparent und auditierbar sind. Dabei wird insbesondere ein ganzheitlicher Ansatz digitaler Resilienz verfolgt, der auch physische Bedrohungen und die Überprüfungen beispielsweise von Lieferanten einbezieht.

> **Für betroffene Institutionen und Unternehmen bedeutet dies, dass sie ihre Prozesse so strukturieren müssen, dass sie jederzeit dahingehend transparent und auditierbar sind.**

### 2.3 European Health Data Space (EHDS)

Mit dem **European Health Data Space (EHDS)** etabliert die EU einen Rahmen für den Austausch und die Nutzung von Gesundheitsdaten. Ziel ist die Stärkung von Forschung, Prävention und Patientenversorgung im europaweiten Rahmen. Die Verordnung gilt dem Grunde nach ab dem 26. März 2027, wobei bestimmte Regeln des EHDS erst zu einem späteren Zeitpunkt gelten. Nachfolgende Kernvorgaben werden zukünftig durch den EHDS gezielt vorangetrieben:

- **Standardisierung medizinischer Datenformate** für europaweite Interoperabilität
- **Grundlagen für solide Sekundärnutzung von Forschungsdaten**
- **Sichere Datenräume** für den Austausch zwischen Einrichtungen, Forschung und Behörden
- **Stärkung der Patientenrechte** durch Transparenz und Zugriff auf eigene Gesundheitsdaten

Für das Gesundheitswesen bedeutet dies einen Paradigmenwechsel: Digitale Prozesse müssen so gestaltet werden, dass sie Daten standardisiert, verschlüsselt und nachvollziehbar handhaben müssen, auch über die bisherigen Anforderungen der DSGVO hinaus.[7]

### 2.4 EU Datenschutz-Grundverordnung (DSGVO)

Die **EU Datenschutz-Grundverordnung (DSGVO)** bleibt ein zentrales Fundament der europäischen Regulierung zur sicheren und vertraulichen personenbezogenen Datenverarbeitung. Bislang ist auch im Zeitraum 2025/2026 zwar keine grundlegende Novellierung der Verordnung vorgesehen, die schon im Mai 2016 in Kraft getreten ist, wohl aber eine **kontinuierliche Konsolidierung in der Praxis**. Dies bedeutet im Einzelnen:

- **Aufsichtsbehörden** setzen verstärkt auf eine einheitliche Auslegung und Durchsetzung bestehender Vorgaben
- Besonders relevant sind Fragen des **rechtskonformen Einsatzes von Cloud-Diensten** und der **Datenübermittlung in Drittländer**
- Zunehmend im Fokus stehen auch **Transparenz- und Rechenschaftspflichten** bei automatisierten Prozessen und beim Einsatz von Künstlicher Intelligenz, auch über eine enge Verzahnung mit der europäischen KI-Verordnung

Für Organisationen in Verwaltung und Gesundheitswesen ergibt sich daraus die Notwendigkeit, ihre Prozesse nicht nur formal, sondern auch praktisch überprüfbar zu dokumentieren und so auszugestalten, dass Datenschutzprinzipien wie Zweckbindung, Datenminimierung und Integrität jederzeit nachweisbar umgesetzt werden.

> **Für Organisationen in Verwaltung und Gesundheitswesen ergibt sich daraus die Notwendigkeit, ihre Prozesse nicht nur formal, sondern auch praktisch überprüfbar zu dokumentieren.**

### 2.5 Digitale Resilienz-Anforderungen für kritische Infrastrukturen

Die Anforderungen an die **digitale Resilienz** von Organisationen mit kritischen Funktionen werden in den kommenden Jahren systematisch ausgeweitet – dies einerseits infolge der gestiegenen Bedrohungslage, aber auch aufgrund der umfassenden Digitalisierung und Vernetzung im industriellen Bereich, welche die bislang klassische Trennung zwischen IT und OT immer weiter erschwert. Maßgeblich ist dabei die Verzahnung mit der **NIS2-Richtlinie**, die verbindliche Cybersicherheitsmaßnahmen und einheitliche Standards für ein

7 Weitere Ausführungen bspws. hier: Buchner/Tinnefeld, in: Kühling/Buchner, DSG-VO BDSG, 4. Aufl. 2024, Art. 89 DSG-VO, Rn. 29.

breites Spektrum von Sektoren vorschreibt und sowohl in Anwendungsbereich wie auch in Inhalt auf der NIS1-Richtlinie aus dem Jahr 2016 fußt. Ergänzend dazu wurden auf europäischer Ebene jedoch auch sektorbezogene Regelwerke, die Resilienzvorgaben weiter konkretisieren und im Zweifelsfall spezialgesetzlich vorrangig anzuwenden sind. Ein Beispiel in diesem Zusammenhang ist der Digital Operational Resilience Act (DORA), der die digitale Widerstandsfähigkeit des Finanzsektor stärken soll.

Zentrale Elemente sind:

- Verpflichtendes Risikomanagement auf technischer und organisatorischer Ebene
- Strukturierte Vorfallmeldungen an nationale und europäische Stellen
- Notfall- und Wiederanlaufpläne, um kritische Dienstleistungen auch im Krisenfall aufrechterhalten zu können
- Regelmäßige Audits und Tests zur Überprüfung der Wirksamkeit implementierter Maßnahmen

**Für öffentliche Verwaltungen, Gesundheitseinrichtungen und andere regulierte Branchen bedeutet dies, dass digitale Prozesse und die Auswahl der eigenen Zulieferer künftig noch stärker auf Nachvollziehbarkeit, Interoperabilität und Sicherheitsmaßnahmen wie Verschlüsselung ausgerichtet werden müssen.**

Für öffentliche Verwaltungen, Gesundheitseinrichtungen und andere regulierte Branchen bedeutet dies, dass digitale Prozesse und die Auswahl der eigenen Zulieferer künftig noch stärker auf **Nachvollziehbarkeit, Interoperabilität und Sicherheitsmaßnahmen wie Verschlüsselung** ausgerichtet werden müssen. Die Verzahnung von Datenschutz, IT-Sicherheit und Resilienzanforderungen erfordert integrierte Ansätze, die sowohl technische Systeme als auch organisatorische Abläufe umfassen.

# 3. Implikationen für die Prozessdigitalisierung & -automatisierung

Diese kursorisch vorgestellten regulatorischen Vorgaben zur digitalen und hybriden Resilienz führen dazu, dass digitale Prozesse nicht mehr ausschließlich unter Effizienz- und Kostengesichtspunkten betrachtet werden können. Organisationen im Gesundheitswesen, in der öffentlichen Verwaltung und in anderen regulierten Branchen müssen ihre Strukturen so gestalten, dass sie rechtskonform, überprüfbar und resilient sind, und insoweit mit der umfassenden Strategie der EU-Gesetzgebung übereinstimmen. Damit verändern sich die Grundanforderungen an **Prozessdigitalisierung und Arbeitsabläufe** in vielen Untenrehmen jetzt und in Zukunft grundlegend.

> **Damit verändern sich die Grundanforderungen an Prozessdigitalisierung und Arbeitsabläufe in vielen Untenrehmen jetzt und in Zukunft grundlegend.**

Im Zentrum steht dabei die Notwendigkeit, Prozesse modular und transparent aufzubauen. Nur wenn einzelne Schritte klar abgegrenzt und dokumentiert sind, lassen sich regulatorische Anforderungen zuverlässig erfüllen und Anpassungen bei künftigen Änderungen des Rechtsrahmens umsetzen. **Transparenz und Auditierbarkeit** sind dabei nicht allein Compliance-Fragen, sondern werden zu einem wesentlichen Bestandteil strategischer Handlungsfähigkeit von Unternehmen in allen Sektoren und Branchen.

Gleichzeitig rückt die sichere Gestaltung von Datenflüssen noch stärker in den Vordergrund. **Ende-zu-Ende-Verschlüsselung** bildet hierfür den Basis-Standard, ergänzt durch differenzierte Modelle des Zugriffs- und Berechtigungsmanagements. Rollenbasierte Zugriffskontrollen stellen sicher, dass sensible Daten ausschließlich von autorisierten Personen eingesehen oder verarbeitet werden können. Dies reduziert Risiken von Datenmissbrauch und unterstützt die Erfüllung zentraler Vorgaben aus der DSGVO und der NIS2-Richtlinie, die sich an dem aktuellen „Stand der Technik“ auszurichten haben.

Ein weiterer entscheidender Aspekt ist die **Nachvollziehbarkeit digitaler Prozesse**. Nur wenn Verantwortlichkeiten eindeutig zugeordnet und Entscheidungen lückenlos dokumentiert werden, können Organisationen ihre Rechenschaftspflichten nach den gesetzlichen Vorgaben zur IT-Sicherheit erfüllen – was im Regelfall schon als Basisanforderung unbedingt vorausgesetzt wird. Gerade im Gesundheitswesen, wo Behandlungsentscheidungen und Datenfreigaben weitreichende Folgen haben, muss die Verbindung zwischen Person, Handlung und Prozessschritt jederzeit klar erkennbar sein.

Darüber hinaus verlangt der europäische Rechtsrahmen eine stärkere Integration digitaler Prozesse in lokale Systeme und eine konsequente **Orientierung an Interoperabilität**. Vorgaben aus dem Data Act und dem European Health Data Space (EHDS) unterstreichen, dass Daten in standardisierten Formaten ausgetauscht und Systeme über Organisationsgrenzen hinweg vernetzt werden müssen, was nicht zuletzt im Hinblick der angestrebten Unabhängigkeit von außereuropäischen Anbietern besondere Gewichtung erlangt. Die Datenwirtschaft der 2020er- und auch der 2030er-Jahre wird im Wesentlichen auf Interoperabilität basieren, was aktuell zugleich auch eine der zentralen Herausforderungen darstellt. Für Verwaltungen, Gesundheitseinrichtungen aber auch andere Unternehmen bedeutet dies, dass Digitalisierung nicht isoliert gedacht werden kann ohne die multifacettierte Anforderungslandschaft mitzudenken. Nur durch die Einbettung in ein interoperables Gesamtgefüge und durch die konsequente Umsetzung klarer digitaler Prozessverantwortlichkeit entsteht die Grundlage für digitale Souveränität. Unternehmen und Institutionen müssen all diese Aspekte also zwingend bei ihrer strategischen Ausrichtung im Blick behalten, um sich rechtssicher, widerstandsfähig und zukunftsfähig aufzustellen.

# 4. Strategische Handlungsempfehlungen

Vor diesem Hintergrund einer zunehmend umfassenden IT-Sicherheitsregulierung entsteht für Entscheidungsträgerinnen und Entscheidungsträger in Gesundheitswesen, Verwaltung und anderen regulierten Branchen die Notwendigkeit, die eigene Digitalisierungsstrategie systematisch an den neuen **Prinzipien der Datensouveränität** auszurichten. Dies erfordert nicht nur die Auswahl einzelner Technologien, sondern die Entwicklung eines strukturierten Kriterienkatalogs, anhand dessen digitale Prozesse gestaltet und bewertet werden können. Im Zentrum stehen dabei Aspekte wie rechtliche Konformität, Sicherheit, Nachvollziehbarkeit und Interoperabilität, die von Beginn an in der Prozessarchitektur berücksichtigt werden müssen.

> **Im Zentrum stehen dabei Aspekte wie rechtliche Konformität, Sicherheit, Nachvollziehbarkeit und Interoperabilität, die von Beginn an in der Prozessarchitektur berücksichtigt werden müssen.**

Ein solcher Kriterienkatalog umfasst sowohl technische als auch organisatorische Dimensionen. Dazu gehört ebenfalls die Gewährleistung einer hohen **Benutzerfreundlichkeit**, da nur intuitiv bedienbare Systeme langfristig Akzeptanz bei Fachanwenderinnen und Fachanwendern finden. Zugleich müssen Barrierefreiheit und inklusive Gestaltung von Prozessen als feste Bestandteile verstanden werden, um eine breite Nutzbarkeit sicherzustellen, wobei dies auch in der Gesetzgebung beispielsweise bereits durch Umsetzung des Barrierefreiheitsstärkungsgesetzes Anklang findet. Überdies bildet die Zugänglichkeit zu Technologie eine Grundvoraussetzung von **„Security by Default“** und **„Privacy by Default“** ab, wie sie durch den EU Cyber Resilience Act (CRA) und die DSGVO wiedergegeben werden. Ergänzend kommt die Fähigkeit hinzu, Dienstleistungen im Self-Service bereitzustellen, wodurch Organisationen die Effizienz steigern und gleichzeitig den Zugang für Bürgerinnen, Patienten oder interne Stakeholder verbessern können.

Damit solche Kriterien nicht abstrakt bleiben, empfiehlt sich die Entwicklung praxisnaher **Checklisten**, die bereits in frühen Phasen der Entscheidungsfindung eingesetzt werden.
Eine solche Checkliste kann beispielsweise folgende Leitfragen enthalten:

- Ist die Benutzerfreundlichkeit des Systems so gestaltet, dass Mitarbeitende ohne umfangreiche Schulung damit arbeiten können?
- Sind Barrierefreiheitsstandards berücksichtigt, sodass auch Menschen mit Einschränkungen gleichberechtigt Zugang haben?
- Werden Self-Service-Funktionalitäten bereitgestellt, die Bürger, Patienten oder interne Stakeholder befähigen, eigenständig auf Services zuzugreifen?
- Ist gewährleistet, dass Datenflüsse durchgehend verschlüsselt und Zugriffskontrollen eindeutig definiert sind?
- Lässt sich die Nachvollziehbarkeit von Prozessen durch Rollenmodelle und Dokumentationspflichten sicherstellen?
- Erfüllt die Lösung die Anforderungen an Interoperabilität und kann sie in lokale Systeme integriert werden?
- Ist eine gewählte Lösung hinreichend cybersicher und nach anerkannten technischen Normen zertifiziert, damit sie den Anforderungen der komplexen und anspruchsvollen regulatorischen Landschaft standhalten kann?

Derartige Prüffragen bieten eine strukturierte Orientierung und schaffen Transparenz in Entscheidungsprozessen. Für Organisationen im öffentlichen Sektor oder im Gesundheitswesen bedeutet dies insbesondere, dass **Ausschreibungen und Vergabeprozesse** von Beginn an auf Datensouveränität ausgerichtet werden müssen. Um diese Anforderung kehrseitig zu erfüllen, sollten auch die sich auf eine Ausschreibung bewerbenden Unternehmen ein Set der relevanten

Prüfmaßstäbe beachten. Wer seine betrieblichen Strukturen rechtzeitig so vorbereitet, dass Nachvollziehbarkeit, Verschlüsselung und Interoperabilität nachweisbar erfüllt sind, verschafft sich nicht nur einen regulatorischen Vorteil, sondern erhöht zugleich die Wettbewerbsfähigkeit in einem zunehmend anspruchsvollen Umfeld.

Nur auf dieser belastbaren Grundlage lassen sich **nachhaltige und strategische Digitalisierungsentscheidungen** treffen, die nicht auf kurzfristige Lösungen setzen, sondern Organisationen dauerhaft in die Lage versetzen, europäische Souveränitätsziele mit eigenen strategischen Interessen zu verbinden und dadurch auf dem Markt erfolgreich zu partizipieren.

# 5. Fazit und Appell zum Handeln

Die digitale Transformation in Europa tritt in eine entscheidende Phase. Schon jetzt und vor allem in den kommenden Jahren ab 2026 werden verbindliche europäische Regelwer-ke die Anforderungen an Datenverarbeitung, Sicherheit und Resilienz deutlich erhöhen. Für Organisationen im Gesundheitswesen, in der öffentlichen Verwaltung und in anderen hochregulierten Branchen bedeutet dies, dass digitale Prozesse nicht länger allein unter dem Gesichtspunkt der Effizienz betrachtet werden können. Rechtskonformität, Nach-vollziehbarkeit und Souveränität entwickeln sich zu grundlegenden Voraussetzungen für die digitale Handlungsfähigkeit über zahllose Branchen hinweg.

Die Analyse der regulatorischen Rahmenbedingungen zur digitalen Resilienz zeigt, dass zentrale Themen wie Ende-zu-Ende-Verschlüsselung, klare Rollenmodelle, modulare Pro-zessarchitekturen und Interoperabilität künftig unverzichtbar sind. Gleichzeitig verdeutli-chen aktuelle Bedrohungslagen, etwa gezielte Cyberangriffe auf kritische Infrastrukturen (KRITIS), dass auch die Widerstandsfähigkeit gegenüber externen Risiken Teil einer nachhaltigen Digitalisierungsstrategie eines jeden Unternehmens und einer jeden öffentli-chen Einrichtung sein muss.

Organisationen sind daher gefordert, ihre digitalen Strukturen bereits heute auf die kom-menden Anforderungen auszurichten. Wer frühzeitig Kriterienkataloge entwickelt, Check-listen etabliert, technisch-organisatorische Maßnahmen umsetzt und Ausschreibungen strategisch vorbereitet, verschafft sich nicht nur einen Vorsprung bei der regulatorischen Absicherung, sondern stärkt zugleich die eigene Position im Wettbewerb um Vertrauen, Sicherheit und Verlässlichkeit.

Der Appell zum Handeln ist deshalb eindeutig: Die Zeit, sich mit den kommenden Anforde-rungen zur digitalen Resilienz und Souveränität auseinanderzusetzen, ist jetzt. Nur durch strukturell abgesicherte und souverän gestaltete digitale Prozesse können Organisationen gewährleisten, dass sie auch in einem zunehmend komplexen geopolitischen und regula-torischen Umfeld rechtssicher agieren, die Kontrolle über ihre Daten behalten und ihre strategische Unabhängigkeit sichern.

## Impressum

**Der Autor**
Der Verfasser Prof. Dr. Dennis-Kenji Kipker ist wissenschaftlicher Direktor am cyberintelligence.institute und Professor für IT-Sicherheitsrecht an der Hochschule Bremen.

*Diese Studie wurde erstellt mit Unterstützung des CII-Fördermitglieds:* FTAPI

---

**cyberintelligence.institute** (Herausgeberin)
MesseTurm
Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.

T +69 5050 34-602

www.cyberintelligence.institute
info@cyberintelligence.institute

---