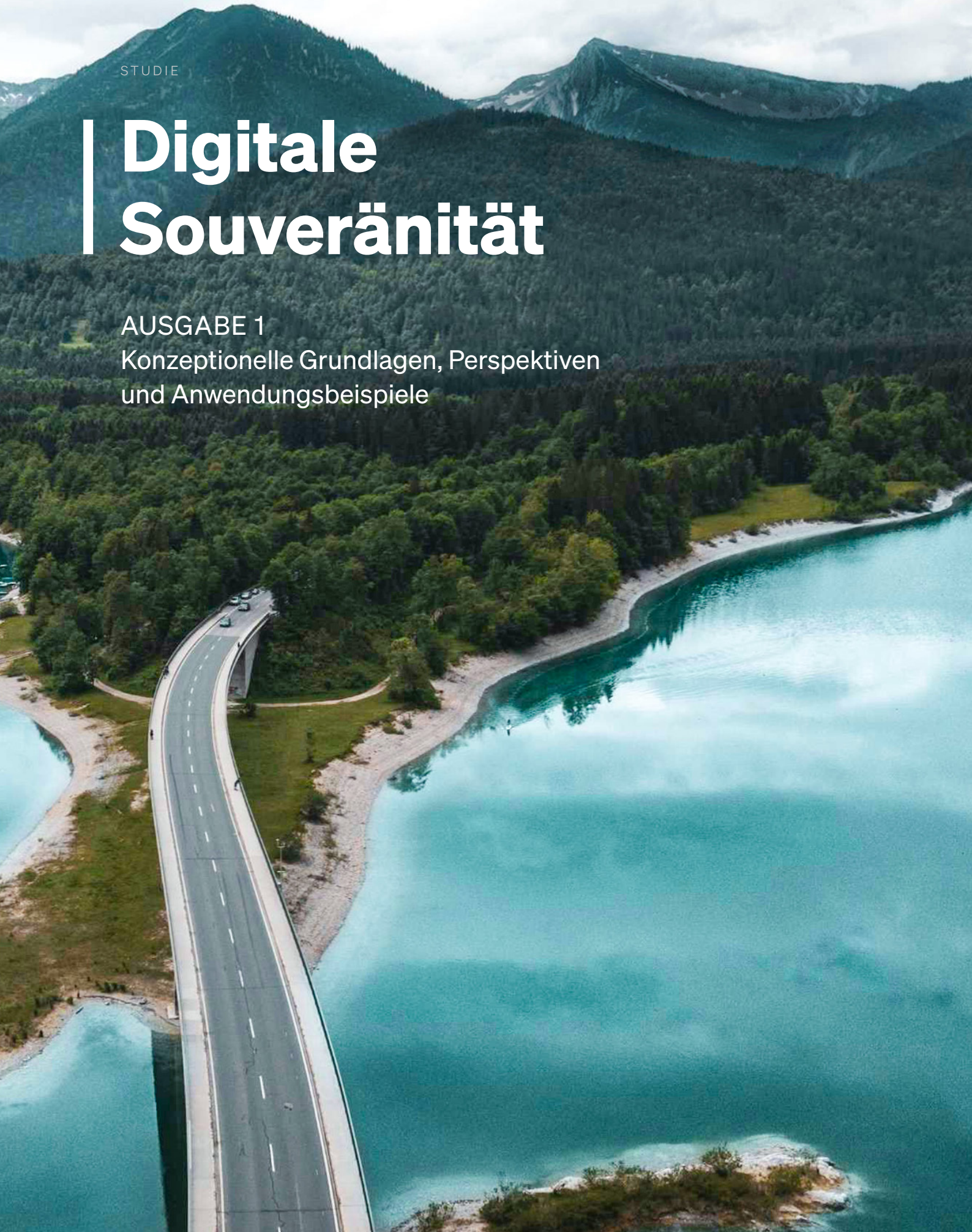
GDV Gesamtverband der Versicherer

BELTIOS

STUDIE

Digitale Souveränität

AUSGABE 1
Konzeptionelle Grundlagen, Perspektiven und Anwendungsbeispiele



GDV

Digitale Souveränität

Herausgeber
Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020–5000, Fax: +49 30 2020–6000
www.gdv.de, berlin@gdv.de

Verantwortlich
Patrik Maeyer
Leiter Betriebswirtschaft, Prozesse und IT
Tel.: +49 30 2020–5452
E-Mail: p.maeyer@gdv.de

Autoren
Florian Baltruschat
Fabian Otto (BELTIOS)
Manuel Audi (BELTIOS)
Patrik Maeyer

Publikationsassistenz
Heike Strauß

Redaktionsschluss dieser Ausgabe
26.11.2024

Disclaimer
Die Analyse stellt eine allgemeine, unverbindliche Information dar. Die Inhalte wurden mit der erforderlichen Sorgfalt erstellt. Gleichwohl besteht keine Gewährleistung auf Vollständigkeit, Richtigkeit, Aktualität oder Angemessenheit der darin enthaltenen Angaben oder Einschätzungen. Eine Verwendung liegt in der eigenen Verantwortung des Lesers.

© GDV 2024

Inhalt

© GDV 2024

Vorwort

Die deutsche Versicherungswirtschaft arbeitet mit Nachdruck an der Modernisierung und Absicherung ihrer Systemlandschaften sowie an der Umsetzung von Potentialthemen wie (generativer) Künstlicher Intelligenz und Open Finance. Cloud Computing ist an vielen Stellen die technologische Grundlage zur Umsetzung dieser Potenziale.

Bei der Wahl der idealen IT-Infrastruktur im Wirrwarr von öffentlichen und privaten Clouds, Branchen-Clouds, eigenen Rechenzentren, Managed-Service-Providern sowie Edge und Multi-Cloud-Architekturen stehen für Entscheider naturgemäß primär Kosten und Nutzen im Mittelpunkt. Doch zunehmend rücken Fragestellungen rund um die eigene digitale Souveränität – im Sinne von Kontrolle über Daten, Prozesse, Technologien, Kosten etc. – ins Zentrum der Betrachtung. Entsprechend reagiert der europäische Technologiemarkt: die ersten souveränen Cloudlösungen entstehen.

Der Umbau der Wertschöpfungsketten geht aus Sicht deutscher Versicherer dabei mit neuen nationalen und internationalen Partnern einher. Anzuerkennen ist, dass derzeit oftmals die technologische Kompetenz außerhalb Deutschlands und Europas liegt. Um die Chancen der Digitalisierung nachhaltig nutzbar zu machen, müssen sich Politik, Unternehmen und Verbraucher daher mit der Frage befassen, wie eine „souveräne“ digitale Transformation aussehen kann bzw. welches Maß an digitaler Souveränität aus verschiedenen Blickwinkeln notwendig oder gewünscht ist.

Das vorliegende Whitepaper ist der erste Teil einer Reihe zum Thema „Digitale Souveränität in der Versicherungswirtschaft“. Die Whitepaper-Reihe wurde in Zusammenarbeit von GDV und BELTIOS erarbeitet und hat zum Ziel, ein Bewusstsein für die oben beschriebene Thematik zu schaffen und Unternehmen dazu zu ermutigen, sich frühzeitig mit der Frage und Ausgestaltung ihrer eigenen digitalen Souveränität zu befassen. Es geht in diesem Kontext nicht darum, eine Strategie der Isolation zu empfehlen oder globale Wertschöpfungsketten grundsätzlich abzulehnen, sondern um anwendungsnahe Hilfestellungen zur Identifikation des eigenen Reifegrads und Bedarfs im Kontext der digitalen Souveränität. Welchen Grad an digitaler Souveränität das jeweilige Unternehmen erreichen möchte, ist dabei Teil der unternehmensindividuellen Geschäftspolitik.

Konkret beschäftigt sich das vorliegende Whitepaper mit den konzeptionellen Grundlagen digitaler Souveränität, Perspektiven zur Versicherungswirtschaft und praxisnahen Anwendungsbeispielen. Zu diesem Zweck wird im ersten Kapitel eine Begriffsdefinition verankert sowie der notwendige Kontext zur Entstehungsgeschichte hergestellt. Die vielfältigen Elemente digitaler Souveränität werden im Anschluss in ein übergeordnetes Rahmenwerk überführt und vervollständigen so die methodischen Grundlagen. Das zweite Kapitel formuliert auf Basis der durchgeführten Experteninterviews fünf Hypothesen zur Rolle digitaler Souveränität in der Versicherungswirtschaft. Konkrete Praxisergebnisse zur Ausgestaltung digitaler Souveränität liefert das dritte Kapitel. Exemplarisch wird anhand einer Versicherungswertschöpfungskette gezeigt, wie sich die Theorie in die Praxis überführen lässt. Als methodischer Ansatz zur Bewertung der eigenen digitalen Souveränität kann das Rahmenwerk zur digitalen Souveränität dienen.

Im Rahmen der Studie, die der Whitepaper-Reihe zugrunde liegt, wurden zunächst explorative Interviews mit Entscheidern aus der deutschen Versicherungsbranche geführt. Die festgestellten Schwerpunktthemen, Problemstellungen und Interessen wurden in der Folge mit einer Reihe von Cloud-Anbietern (AWS, Microsoft, Google Cloud, IBM, OVHcloud, IONOS) diskutiert und in die vorliegenden Ergebnisse überführt.

© GDV 2024

1. Begriffsdefinition: Was bedeutet digitale Souveränität?

Ein Konzept noch ohne einheitliche Definition

Die Bundesdruckerei leistet als Technologieunternehmen des Bundes einen Beitrag für die digitale Souveränität Deutschlands und Europas und stellte im Jahr 2020 im Zuge der strukturierten Auseinandersetzung mit digitaler Souveränität fest: „Eine feststehende Definition des Begriffs gibt es nicht."[1] Dieser Sachverhalt hat sich bis heute nicht geändert: Ideen zu digitaler Souveränität unterscheiden sich je nach thematischem bzw. geografischem Kontext und eine Legaldefinition von digitaler Souveränität existiert zum Zeitpunkt der Erstellung dieses Whitepapers nicht.

Im Bewusstsein der vielfältigen co-existierenden Auslegungen des Begriffs soll diesem Whitepaper dennoch ein einheitliches Verständnis zugrunde gelegt werden. Praxisgerecht erscheint daher die Definition aus der Datenstrategie der Bundesregierung, die wir auf Basis unserer Erfahrungen aus der Interview-Reihe um zusätzliche Aspekte erweitern:

> Digitale Souveränität beschreibt die Fähigkeit von Staaten, Unternehmen und Verbrauchern, die digitale Transformation selbstbestimmt zu gestalten. Digital souverän zu sein bedeutet im Rahmen des geltenden Rechts unabhängig zu entscheiden, in welchen Bereichen und unter welchen Bedingungen technologische, operative und Daten-Souveränität erwünscht oder notwendig ist. Grundlage für die Ausübung digitaler Souveränität sind umfangreiche digitale Kompetenzen.[2]

Digitale Souveränität ist ein noch junges Thema

Das Konzept der digitalen Souveränität leitet sich von der nationalen Souveränität ab, hat sich jedoch im digitalen Zeitalter auf die Kontrolle digitaler Infrastrukturen, Daten und Technologien ausgeweitet.

Als Erweiterung des klassischen geographischen Raums stellt der digitale Raum mittlerweile eine kritische Funktion für die nationale Sicherheit und wirtschaftliche Stabilität dar.

In einer zunehmend vernetzten und geopolitisch komplexen Welt trägt digitale Souveränität dazu bei, die Abhängigkeit von externen Technologieanbietern zu reduzieren, das Risiko von Datenverlust und Cyberangriffen zu minimieren und regulatorische Vorgaben einzuhalten. Sie stärkt zudem die Innovationskraft und schützt strategische Informationen – beides zentrale Erfolgsfaktoren in der digitalen Wirtschaft.

Der Bedeutungszuwachs der digitalen Souveränität ist jedoch ein Phänomen der jüngeren Vergangenheit. Trendanalysen zeigen, dass das Interesse an digitaler Souveränität mit technologischen Entwicklungen wie Cloud Computing oder Künstliche Intelligenz korreliert. Seit 2020 tragen auch geopolitische Ereignisse zu einem verstärkten Fokus auf digitale Unabhängigkeit bei.

Kernelemente digitaler Souveränität

Als Grundlage dieses Whitepapers und der nachfolgenden Anwendung des Konzepts der digitalen Souveränität auf die Versicherungswirtschaft dienen einige Kernelemente (vgl. Abb. 1 auf S. 6).

Betrachtungsobjekte

Heute wird die digitale Souveränität als eine kritische strategische Herausforderung angesehen – nicht nur für Staaten, sondern auch für Unternehmen, die ihre Daten schützen, ihre Wettbewerbsfähigkeit erhalten und sich in der komplexen Landschaft digitaler Ökosysteme zurechtfinden wollen. Auch für Verbraucher ist das Thema relevant. Digitale Souveränität für Verbraucher bedeutet, die Kontrolle über persönliche Daten und die Entscheidungsmacht darüber zu haben, wie, wo und von wem diese Daten genutzt werden.

1 Bundesdruckerei, 2020
2 GDV & BELTIOS in Anlehnung an Datenstrategie der Bundesregierung, 2021

© GDV 2024

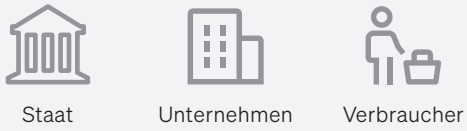
Digitale Souveränität als mehrdimensionales Konzept

Abbildung 1 · Kernelemente zum Konzept der digitalen Souveränität

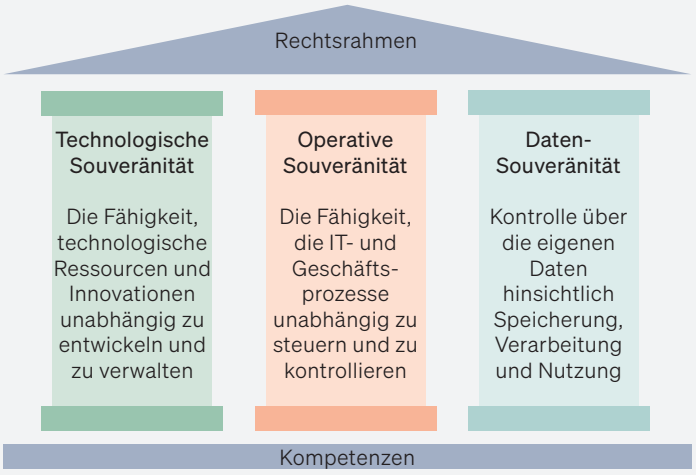
Definition

Sie beschreibt die Fähigkeit von Staaten, Unternehmen und Verbrauchern, die digitale Transformation selbstbestimmt zu gestalten. Digital souverän zu sein bedeutet im Rahmen des geltenden Rechts unabhängig zu entscheiden, in welchen Bereichen und unter welchen Bedingungen technologische, operative und Daten-Souveränität erwünscht oder notwendig ist. Grundlage für die Ausübung digitaler Souveränität sind umfangreiche digitale Kompetenzen.

Betrachtungsobjekte



Bestandteile



Trade-Offs

Quelle: GDV & BELTIOS in Anlehnung an Datenstrategie der Bundesregierung, 2021

Bestandteile

Digitale Souveränität setzt sich aus mehreren Elementen zusammen. Wir interpretieren diese Elemente bildlich als Haus: Der geltende Rechtsrahmen bildet das Dach. Die Kompetenzen, die – unabhängig vom Betrachtungsobjekt – notwendig sind, um die eigene digitale Souveränität zu erhöhen, bilden das Fundament. Schließlich gibt es drei zentrale Säulen digitaler Souveränität: technologische Souveränität, operative Souveränität und Datensouveränität.

Trade-offs

Im Kontext der digitalen Souveränität spielen letztlich Trade-offs eine wesentliche Rolle, da sie die Notwendigkeit verdeutlichen, zwischen verschiedenen, oft widersprüchlichen Zielen eine Balance zu finden. Die Entscheidung für mehr digitale Unabhängigkeit und Kontrolle ist selten ohne Kompromisse zu erreichen, und diese Abwägungen beeinflussen die strategischen Entscheidungen erheblich. Bei der Umsetzung digitaler Souveränität müssen daher verschiedene Faktoren gegeneinander abgewogen werden, darunter beispielsweise: Leistungsfähigkeit, Unabhängigkeit und Kosten.

Entscheidungsträger sehen sich mit einem Trilemma konfrontiert, denn es ist nicht immer möglich, alle Faktoren gleichermaßen zu optimieren. Hinsichtlich der Ausgestaltung von digitaler Souveränität lässt sich vereinfacht eine Bandbreite aus den nachfolgenden Handlungsoptionen abstecken:

© GDV 2024

- **Unabhängigkeit bei hoher Leistungsfähigkeit:** In dieser Kombination wird eine unabhängige IT angestrebt, die eine hohe Leistungsfähigkeit aufweist. Praktisch bedeutet dies den weitreichenden Verzicht auf Sourcing-Strategien zugunsten von Inhouse-Entwicklungen und Inhouse-Betrieb. Um diese beiden Ziele zu erreichen, müssen erhebliche finanzielle Mittel investiert werden, was die Kosten in die Höhe treibt.

- **Leistungsfähigkeit bei niedrigen Kosten:** Der etablierte und weit verbreitete Min-Max-Gedanke spiegelt sich in diesem Ansatz wider. Die größtmögliche Leistungsmenge soll mit den geringstmöglichen Kosten erzielt werden. Aufgrund von Faktoren wie Spezialisierungen, Skaleneffekten und Standortvorteilen führt die konsequente Umsetzung dieser Zielstellung dazu, dass die eigene Sourcing-Strategie gegenüber Dritten geöffnet werden muss. Vorbehaltlich weiterer Maßnahmen zur Stärkung der digitalen Souveränität hat dieser Ansatz in seiner Reinform zur Folge, dass die digitale Souveränität des Unternehmens gegenüber dem Dritten abnimmt.

- **Unabhängigkeit bei niedrigen Kosten:** Ein hohes Maß an Unabhängigkeit bei gleichzeitig geringen Kosten kann nur erreicht werden, wenn auf die Maximierung der Leistungsfähigkeit verzichtet wird. Bei dieser Strategie liegt der Schwerpunkt demnach auf Inhouse-Entwicklungen und einem Inhouse-Betrieb zur Steigerung der Unabhängigkeit. Da gleichzeitig die Kosten gering bleiben soll, kann jedoch nicht die gleiche Leistungsfähigkeit erreicht werden wie bei einem Drittanbieter mit einer Spezialisierungsstrategie.

Die Relevanz dieser Trade-offs liegt darin, dass sie helfen, die Komplexität und die Konsequenzen der Entscheidungen im Streben nach digitaler Souveränität besser zu verstehen und zu managen. Außerdem verdeutlichen sie, dass Souveränität im digitalen Raum mehr ist als ein Synonym für Unabhängigkeit.

© GDV 2024

2. Digitale Souveränität: Perspektiven zur Versicherungswirtschaft

Im Rahmen der diesem Whitepaper zugrundeliegenden Studie wurden mehr als 30 Gespräche mit verschiedenen Versicherern (vorrangig Vertreter der IT-Organisationen), Technologie-Experten und Cloud-Anbietern (AWS, Google Cloud, Microsoft, IBM, OVHcloud, IONOS) geführt. Aus den aggregierten Interviews werden in der Folge fünf Hypothesen als Perspektiven zur Versicherungswirtschaft zum Thema digitale Souveränität abgeleitet und diskutiert.

> 1. Viele Versicherer befassen sich unbewusst bereits intensiv mit digitaler Souveränität.

Der Begriff der digitalen Souveränität taucht selten in Befragungen von Versicherungsunternehmen nach ihren strategischen Prioritäten oder Herausforderungen auf. Mit großer Wahrscheinlichkeit liegt das an der Tatsache, dass eine einheitliche Begriffsdefinition nicht existiert und die diversen Aspekte digitaler Souveränität selten als ganzheitliches Konstrukt betrachtet werden. Denn viele der im Rahmen dieser Studie befragten Versicherer beschäftigen sich bereits mit digitaler Souveränität, sie überschreiben ihre Initiativen nur nicht so. Als hoch regulierte Industrie, die viele sensible Daten verarbeitet, spielt bspw. Datensouveränität bei den Branchenvertretern eine große Rolle. Das Streben nach der Erfüllung regulatorischer Anforderungen dominiert. Aber auch die Vermeidung bzw. Reduzierung von Vendor Lock-ins (insb. im Cloud-Umfeld) beschäftigt die befragten Versicherer. Es gibt jedoch auch vereinzelt Ausnahmen von Versicherern, die eine IT-Strategie mit Fokus auf der eigenen Souveränität definiert haben und nun erfolgreich umsetzen.

Es stellt sich die Frage, welche Potenziale sich zusätzlich heben ließen, wenn digitale Souveränität als ganzheitliches Konzept verstanden würde und explizite „Souveränitäts-Ziele“ definiert würden. Welchen ökonomischen Wert kann digitale Souveränität schaffen? Kann das Trilemma aus Leistungsfähigkeit, Unabhängigkeit und Kosten potenziell aufgelöst werden?

> 2. Digitale Souveränität kann als Befähiger und Beschleuniger der eigenen digitalen Transformation genutzt werden.

Eine Teilantwort auf die Frage nach dem ökonomischen Wert von digitaler Souveränität könnte das Verständnis des Konzepts als Befähiger und Beschleuniger von digitaler Transformation liefern. Dass Versicherer bspw. bei der Modernisierung ihrer Kernsysteme und der Nutzung von Cloud Technologie im Vergleich zu anderen Branchen konservativer sind, bestätigt sich auch in den im Rahmen dieser Studie geführten Interviews. Oft werden Kontroll-Aspekte priorisiert behandelt (vgl. Trilemma Leistungsfähigkeit vs. Unabhängigkeit vs. Kosten). Hinzu kommt, dass Versicherer als hochregulierte Unternehmen für den regelkonformen Betrieb der IT verantwortlich sind und daher mit großer Sorgfalt agieren. Auch die befragten Cloud-Anbieter weisen auf heterogene Reifegrade in Abhängigkeit der Größe der Versicherer hin: bspw. wird globalen Playern eine höhere digitale Souveränität als kleinen deutschen Versicherern bescheinigt.

Wenn Versicherer digitale Souveränität als selbstbestimmte Kombination von Leistungsfähigkeit und Kontrolle betrachten und nicht mit maximaler Unabhängigkeit gleichsetzen, können die Nutzung neuer Technologien und die digitale Transformation effektiver gelingen.

> 3. Die Sicherheit und Verlässlichkeit von On-Premise Bestandsverwaltungen kann in einer dynamischen Umgebung an ihre Grenzen stoßen.

Die Bestandsverwaltung ist eine der Kernaktivitäten eines jeden Versicherers. Es ist verständlich und im Interesse des Kunden, dass im Umgang mit solch sensiblen und geschäftskritischen Daten höchste Vorsicht geboten ist. Es ist ebenso angemessen, dass viele der befragten Versicherer aus diesem Grund einen großen Teil der Systeme in eigenen Rechenzentren verwalten. Kontrolle und Datenhoheit führen zu voller

© GDV 2024

Verantwortung für alle operativen und sicherheitsrelevanten Entscheidungen rund um den eigenen Bestand. Dennoch gibt es auch Risiken bei einer On-Premise Bestandsverwaltung: Durch massiv steigende Anforderungen im Bereich von Cybersecurity wird es immer anspruchsvoller und kostenintensiver, Sicherheitsvorkehrungen, wie sie bspw. von Cloud-Anbietern bereitgestellt werden, in eigenen Rechenzentren nachzuhalten. Außerdem begeben sich Versicherer in eine hohe Abhängigkeit von Ressourcen und Expertise, um die Systeme selbst instandzuhalten und weiterzuentwickeln. Nicht zuletzt sind geopolitische Entwicklungen bei Datenspeicherung an einzelnen Standorten zumindest zu beachten.

Es stellt sich die Frage, was eine souveräne Bestandsverwaltung wirklich bedeutet und in welcher Ausgestaltung ein idealer Kompromiss von „make“ und „buy“ getroffen werden kann. Kann ein Hybrid-Ansatz eine Lösung sein, bei dem nach individueller Prüfung selektiert wird, welche Daten und Workloads on-Premise und welcher in der Cloud betrieben werden? (u. a. Trennung von Daten verschiedenen Schutzklassen und Zusammenführung im Frontend des berechtigten Nutzers) Welche Rolle spielt Standard-Software in diesem Zusammenhang?

> 4. Schon heute haben Versicherer eine Vielzahl direkter und indirekter Beziehungen zu Cloud-Diensten.

Unabhängig davon, welchen Reifegrad Versicherer in Bezug auf die eigene Cloud Journey bzw. Strategie haben: Auf die Nutzung von Software-as-a-Service und APIs zu externen Cloud-basierten Datenquellen und Plattformen können und möchten die wenigsten Versicherungsunternehmen gänzlich verzichten. Durch regulatorische Anforderungen wie bspw. durch das FIDA-Rahmenwerk wird die Öffnung der eigenen Systeme für einige Bereiche in absehbarer Zukunft sogar zur Verpflichtung. Während die FIDA-Regulierung und Open Insurance allgemein die digitale Souveränität von Versicherungsnehmern, also meist natürlichen Personen, stärken soll, haben die vielfältigen und neu entstehenden indirekten Beziehungen von Versicherern (Dateninhabern) zu Anbietern von Produkten und Dienstleistungen (Datennutzern) natürlich auch einen Einfluss auf die digitale Souveränität der Versicherungsunternehmen selbst. Cloud-Anbieter, die das zur Verfügung stellen der Daten in der Regel ermöglichen, komplettieren das Bild. Vielen befragten Versicherern ist die Notwendigkeit einer strategischen Einordnung bewusst, gleichzeitig unterschätzen viele der befragten Versicherer, wie fundamental Cloud-Dienste schon heute den Versicherungsalltag bestimmen (z. B. digitale Signatur, Ausweiserkennung, Bonitätsprüfung) und dass dies perspektivisch eher zunehmen als abnehmen wird.

Wenn Versicherer digitale Souveränität zu einem integralen Bestandteil der IT-Strategie machen, gewinnt die Organisation an Transparenz, Selbstbestimmtheit und unternehmerischer Handlungsfähigkeit. Auch die Geschwindigkeit, mit der regulatorische Anforderungen umgesetzt und technische Innovationen genutzt werden können, nimmt potenziell zu.

> 5. Durch einen zu großen Fokus auf Regulatorik und Compliance können Chancen am Markt versäumt werden.

Im Vergleich der Versicherungsunternehmen lässt sich eine Heterogenität bzgl. der bewussten Beschäftigung mit digitaler Souveränität beobachten. Größtenteils übereinstimmend kann ein Fokus in der operativen Auseinandersetzung von Versicherern mit dem Konzept digitaler Souveränität auf das Einhalten regulatorischer Anforderungen und das Vermeiden von zu großen externen Abhängigkeiten und ungewollten Zugriffen festgestellt werden. Globale Player sind naturgemäß kleinen und mittelgroßen deutschen Versicherern bei der digitalen Transformation und dem Verständnis und der Umsetzung digitaler Souveränität etwas voraus.

Die pragmatische und chancenorientierte Auseinandersetzung mit digitaler Souveränität, u. a. durch den Einsatz von Multi-Cloud-Strategien, Verschlüsselungstechnologien und Open-Source-Software kann zur Erhöhung der eigenen Leistungsfähigkeit bei Wahrung der digitalen Unabhängigkeit und Selbstbestimmtheit führen. Wie hoch die Reifegrade der Versicherer tatsächlich sind, gilt es jedoch noch zu untersuchen – z. B. mit dem „Digitale Souveränitäts-Score“ (siehe nachfolgendes Kapitel).

© GDV 2024

3. Die praktische Anwendung von digitaler Souveränität

Die drei Säulen digitaler Souveränität im Unternehmenskontext

Angewendet auf das Unternehmen als Betrachtungsobjekt, adressiert jede der drei Säulen digitaler Souveränität spezifische Herausforderungen in einer zunehmend vernetzten und globalisierten Wirtschaft. Nachfolgend werden einige Aspekte näher beleuchtet, die aus Unternehmensperspektive zu beachten sind, um das eigene Geschäft möglichst digital souverän auszurichten, (vgl. Tabelle 1). Die folgenden Definitionen werden dafür zugrunde gelegt:

- → **Technologische Souveränität:** Die Fähigkeit, technologische Ressourcen und Innovationen unabhängig zu entwickeln und zu verwalten.
- → **Operative Souveränität:** Die Fähigkeit, IT- und Geschäftsprozesse unabhängig zu steuern und zu kontrollieren.
- → **Datensouveränität:** Die Kontrolle über die eigenen Daten hinsichtlich Speicherung, Verarbeitung und Nutzung.

Die drei Säulen der digitalen Souveränität im Unternehmenskontext

Tabelle 1 · Techologische, operative und Daten-Souveränität

Aspekt	Ausprägung im Unternehmenskontext
Technologische Souveränität	
Software-Entwicklung & -Wartung	Unternehmen verfügen über die Fähigkeit, maßgeschneiderte Softwarelösungen intern zu entwickeln, anzupassen und kontinuierlich zu warten. Diese Kompetenz ermöglicht es, spezifische und sich ändernde Geschäftsanforderungen optimal zu erfüllen.
Technologische Unabhängigkeit	Durch die Reduzierung der Abhängigkeit von externen Technologieanbietern und proprietären Lösungen können Unternehmen die Kontrolle über ihre IT-Infrastruktur und -Strategien bewahren. Dies verringert Risiken, die mit externen Abhängigkeiten verbunden sind und ermöglicht eine flexible Anpassung der technologischen Mittel an sich verändernde Bedürfnisse.
Offene Standards & OSS	Unternehmen fördern aktiv die Verwendung weit akzeptierter Protokolle, offener Standards und Open-Source-Software (OSS). Dies erhöht die Interoperabilität und trägt (zumindest theoretisch) zur Reduzierung der technologischen Abhängigkeiten und Erhöhung der Flexibilität bei.
Innovation & Forschung	Unternehmen sind in der Lage, eigene technologische Lösungen und Innovationen zu entwickeln und erfolgreich zu implementieren. Kontinuierliche Weiterentwicklung und Wettbewerbsvorteile können gestärkt werden, indem fortschrittliche Technologien und maßgeschneiderte Lösungen eingeführt werden.
Lieferkettenkontrolle	Durch die Kontrolle und Sicherstellung der Sicherheit und Vertrauenswürdigkeit der technologischen Lieferketten können Unternehmen die Integrität und Zuverlässigkeit ihrer Technologieinfrastruktur gewährleisten. Dies minimiert das Risiko von Sicherheitsvorfällen und gewährleistet die Kontinuität des Geschäftsbetriebs.

© GDV 2024

Aspekt	Ausprägung im Unternehmenskontext
Operative Souveränität	
Kritische Infrastruktur	Unternehmen gewährleisten die Kontrolle über alle wesentlichen Infrastrukturen und deren Lieferanten / Betreiber, die für den operativen Betrieb unerlässlich sind (z. B. Server, Netzwerke, Rechenzentren und Versorgungsnetze). Diese Kontrolle sichert nicht nur die Betriebsabläufe, sondern schützt auch vor Cyberbedrohungen, indem robuste Sicherheitsmaßnahmen implementiert werden, um die Integrität und Verfügbarkeit dieser kritischen Systeme zu gewährleisten.
Resilienz & Kontinuitätsplanung	Unternehmen entwickeln und implementieren umfassende Strategien und Pläne, um den Betrieb im Falle von Störungen oder Ausfällen aufrechtzuerhalten (z. B. durch Notfallpläne und Redundanzlösungen).
Vendoren-Unabhängigkeit	Durch die gezielte Reduzierung der Abhängigkeit von externen Anbietern können Unternehmen Lock-in-Effekte vermeiden und ihre operative Flexibilität maximieren. Dies ist besonders relevant im Kontext der Cloud-Strategie, z. B. bei der Wahl und bedarfsgerechten Verwaltung und Nutzung von Cloud-Dienstmodellen.
Compliance & Regulierung	Unternehmen stellen sicher, dass alle relevanten gesetzlichen und regulatorischen Anforderungen durch Lieferanten und das Unternehmen selbst eingehalten werden. Dies umfasst die Implementierung von Richtlinien und Prozessen zur kontinuierlichen Überwachung und Anpassung an regulatorische Änderungen, um rechtliche Risiken zu minimieren und die Integrität der betrieblichen Abläufe zu gewährleisten.
Transparenz	Durch Transparenz über alle internen Prozesse, Technologien und Daten bewahren Unternehmen ihre strategische und operative Entscheidungshoheit. Diese Selbstbestimmung ermöglicht eine unabhängige und flexible Entscheidungsfindung, ohne auf externe Parteien oder Dienstleister angewiesen zu sein.
Kostenkontrolle	Durch die vollständige Transparenz und proaktive Steuerung der IT- und Betriebskosten können Unternehmen ihre finanzielle Handlungsfähigkeit maximieren (Optimierung von IT-Ressourcen, Flexibilität bei der Skalierung, Fixkosten-Reduktion & verursachungsgerechte Schlüsselung auf Geschäftsvorfälle sowie langfristige Planbarkeit von Investitionen / Betriebskosten). Besonders relevant ist dies im Hinblick auf die Minimierung unerwarteter Kosten und die effiziente Ausrichtung der IT-Ausgaben an den strategischen Zielen des Unternehmens.
Datensouveränität	
Datenschutz	Unternehmen gewährleisten die Einhaltung aller relevanten Datenschutzgesetze (z. B. DSGVO oder BDSG) und anderer internationaler Vorschriften (z. B. DORA mit Fokus auf Cyber-Resilienz). Es wird sichergestellt, dass alle rechtlichen Implikationen erkannt und berücksichtigt werden, um den Schutz der personenbezogenen Daten umfassend zu gewährleisten.
Datenhoheit	Unternehmen sorgen dafür, dass alle Daten in der Kontrolle der Organisation bleiben und vor unbefugtem Zugriff oder Abfluss geschützt sind. Dies umfasst die Implementierung von Kontrollmechanismen und Prozessen, um die Vertraulichkeit und Exklusivität der Unternehmensdaten zu wahren.
Datenintegrität & -sicherheit	Es werden umfassende Maßnahmen zum Schutz der Daten vor Verlust, Manipulation und unberechtigtem Zugriff getroffen. Diese Maßnahmen umfassen sowohl technische Sicherheitsvorkehrungen als auch organisatorische Prozesse, um die Integrität und Sicherheit der Daten kontinuierlich zu gewährleisten.
Datenzugriff & -verwaltung	Unternehmen implementieren rigorose Zugriffs- und Verwaltungskontrollen, um sicherzustellen, dass nur autorisierte Personen Zugang zu sensiblen Daten erhalten. Dies umfasst die Einrichtung von klaren Berechtigungsstrukturen und die regelmäßige Überprüfung der Zugriffskontrollen, um die Sicherheit und Vertraulichkeit der Daten zu wahren. Ebenso umfasst dies Mechanismen zur Herausgabe von Daten an die Eigentümer der Daten sowie die Löschung von Daten, wenn die Grundlage zur Aufbewahrung nicht mehr gegeben ist.
Datenstandort	Die Kontrolle über den physischen Speicherort der Daten wird durch die sorgfältige Auswahl der Rechenzentren und die Einhaltung der rechtlichen Anforderungen des jeweiligen Speicherlandes sichergestellt. Unternehmen stellen sicher, dass alle geltenden gesetzlichen Anforderungen erfüllt werden, um rechtlichen und regulatorischen Risiken vorzubeugen.
Datenportabilität & -interoperabilität	Unternehmen können ihre Daten unabhängig von spezifischen Systemen oder Anbietern flexibel nutzen und transferieren. Besonders relevant ist dies bei der Integration unterschiedlicher IT-Systeme und der Vermeidung von Anbieterabhängigkeiten, um eine reibungslose Datenmigration und -nutzung zu gewährleisten.

Quelle: GDV & BELTIOS

© GDV 2024

Vorteile und Anwendungsbeispiele digitaler Souveränität

Abbildung 2 · Die praktische Bedeutung von Digitaler Souveränität entlang der Versicherungswertschöpfungskette

Versicherungsunternehmen, die ein hohes Maß an digitaler Souveränität aufweisen, können beispielsweise:

Produktentwicklung	→ präzise auf Änderungen im Geschäftsumfeld reagieren und in selbstbestimmter Geschwindigkeit uneingeschränkt maßgeschneiderte, innovative Produkte entwickeln. → durch die Integration von gesetzlichen Anforderungen in den Produktentwicklungsprozess sicherstellen, dass Tarife regulatorisch konform sind und dadurch Haftungsrisiken minimieren. → durch die Nutzung von internen Daten Kundenbedürfnisse und Markttrends erkennen und einen Wettbewerbsvorteil erzielen. → auf Basis einer entsprechenden Rechtsgrundlage datengetriebene Finanzdienstleistungen oder personalisierte Produkte für den Kunden anbieten.
Marketing, Vertrieb & Kundenservice	→ schneller auf spezifische Kundenanforderungen im Kundendienst und Vertrieb reagieren, indem bspw. CRM-Systeme mit neuen Kommunikationskanälen (z. B. Chatbots) und Marketing- und Vertriebsplattformen integriert werden. → flexibel und ohne zu große Abhängigkeit zu einzelnen Vendoren die stets beste Software wählen, um in Marketing und Vertrieb auf Markttrends und sich wandelnde Kundenanforderungen zu reagieren. → sicherstellen, dass im Kundendienst ausschließlich entsprechend autorisierte Mitarbeitende Zugriff auf sensible Kundeninformationen haben. → gegenüber den Kunden transparent machen, wo und unter welchen Bedingungen Daten verarbeitet werden.
Risikoprüfung & Tarifierung	→ eigene Algorithmen und KI-basierte Systeme zur Optimierung des Underwritings und der Risikobewertung entwickeln. → schnell und regelmäßig Anpassungen an Risikobewertungsmodellen vornehmen, um Haftungs- und Compliance-Risiken zu reduzieren. → die Integrität der Daten gewährleisten, die für Risikomodelle und Prämienkalkulation verwendet werden, um genaue und verlässliche Entscheidungsgrundlagen im Underwriting und der Risikobewertung zu sichern.
Vertragsverwaltung	→ zielgerichtet wiederkehrende Prozesse automatisieren und dadurch Fehlerquellen reduzieren, Effizienz in der Verwaltung steigern und Reaktionsgeschwindigkeit auf (Kunden-) Anfragen erhöhen. → Änderungen in Vertragsbedingungen schnell implementieren und effiziente Prozesse in Verwaltungsaufgaben sicherstellen. → das Risiko eines unkontrollierten Datenabflusses minimieren.
Schaden & Leistung	→ sich durch die Nutzung offener Standards leichter mit externen Partnern (z. B. Werkstätten, Gutachtern) integrieren und somit ein effizienteres Schadenmanagement betreiben und erhöhte Kundenzufriedenheit ermöglichen. → auch bei Systemausfällen oder Krisen sicherstellen, dass Schadenregulierungen fortgeführt und Kundenanfragen weiter bearbeitet werden können. → verhindern, dass manipulierte Daten zur Schadenregulierung verwendet werden.
Rückversicherung	→ eigene Simulationen von Katastrophenszenarien und deren Auswirkungen auf das Risikoprofil erstellen, um unabhängig angemessene Rückversicherungsdeckungen festzulegen und bessere Verhandlungspositionen zu erlangen. → gezielt entscheiden, welche Informationen mit Rückversicherern zur Optimierung von Vertragskonstellationen geteilt werden.
Unterstützende Aktivitäten (IT, Personal, Risikomanagement und Kapitalanlage, ...)	→ externe Sicherheitsrisiken im IT- und Datenmanagement reduzieren und/oder sogar sogenanntes De-Platforming vermeiden (ein Technologieanbieter verfügt über den „Killswitch“ zum Abschalten ganzer Anwendungen und Infrastrukturen). → Abhängigkeiten von proprietären Risikomanagement Tools vermeiden, eigene Risikomodelle entwickeln und anpassen und dadurch Wettbewerbsvorteile erreichen. → Technologie-Know-How und -Expertise aufbauen und dadurch Abhängigkeiten gegenüber Drittanbietern reduzieren und Budgets für externe Berater zielgerichteter zur Differenzierung verwenden.

Quelle: GDV & BELTIOS

© GDV 2024

Digitale Souveränität entlang der Versicherungswertschöpfungskette

Die Abbildung 2 zeigt die praktische Bedeutung von digitaler Souveränität entlang der Versicherungswertschöpfungskette. Die Auflistung hat explizit keinen Anspruch auf Vollständigkeit, sondern soll lediglich einige Anwendungsbeispiele skizzieren, die mit einem hohen Maß an digitaler Souveränität aus der Perspektive eines Versicherungsunternehmens erreicht werden können.

Bewertung digitaler Souveränität

Mit dem „Digitale Souveränitäts"-Rahmenwerk (vgl. Abb. 3) werden die vorangegangen konzeptionellen Grundlagen digitaler Souveränität in einem praxisgerechten Werkzeug zusammengeführt. Dieses Werkzeug kann von Unternehmen dazu verwendet werden, die eigene digitale Souveränität zu ermitteln und entlang der drei beschriebenen Säulen zu bewerten. Das Rahmenwerkl unterstützt Entscheidungsträger dabei, ihre eigene Organisation im Status Quo zu analysieren und erste strategische Handlungsfelder zu identifizieren, um einzelne Teilaspekte digitaler Souveränität zu optimieren. Wichtig ist, dass höhere digitale Souveränität nicht zwangsläufig höhere Unabhängigkeit oder vermeintlich souveräne Einzelfall-Entscheidungen für bspw. On-Premise Infrastruktur bedeutet. Digitale Souveränität bedeutet vielmehr Bewusstsein und klar definierte Strategien entlang der untersuchten Kategorien; dies kann auch das Eingehen von Abhängigkeiten zur Steigerung der Leistungsfähigkeit bzw. Senkung der Kosten einschließen. Schließlich erfolgt eine Beurteilung stets unternehmensindividuell und die Bewertung ist im Abgleich mit eigenen Zielen und Strategien vorzunehmen.

Exemplarische Darstellung des Rahmenwerks zu digitaler Souveränität

Abbildung 3 · Modell zur Ermittlung der digitalen Souveränität von Versicherungsunternehmen

Quelle: GDV & BELTIOS

© GDV 2024

4. Fazit & Ausblick

Diese erste Ausgabe der Whitepaper-Reihe zum Thema „Digitale Souveränität in der Versicherungswirtschaft“beschäftigt sich mit konzeptionellen Grundlagen zum Thema und adressiert damit den Aufklärungsbedarf der Industrie. Aus der Diskussion der Perspektiven zur Versicherungswirtschaft wird deutlich, was schon in der Ausarbeitung der Trade-offs theoretisch hergeleitet wurde: Digitale Souveränität ist ein komplexes Konzept mit vielen Facetten, das bei ganzheitlicher Betrachtung mehr bedeutet als „nur“ Unabhängigkeit im digitalen Raum. Ein Unternehmen kann bspw. auch dann digital souverän sein, wenn es die eigenen Abhängigkeiten kennt und ggf. sogar bewusst und in Abwägung von anderen Faktoren (wie bspw. Leistungsfähigkeit und Kosten) eingeht. Eine fundamentale Verbindung zur Unternehmensstrategie besteht.

Digitale Souveränität ist auch deswegen ein komplexes Konzept, da es sich nicht auf einzelne Unternehmensbereiche oder Funktionen beschränkt. Die drei Säulen digitaler Souveränität zeigen bspw. die Relevanz in technologischen und operativen Fragestellungen sowie dem subjektiv am weitest entwickelten Themenbereich rund um die unternehmenseigene Datenhaltung. Im Kontext der digitalen Transformation von Versicherungsunternehmen spielt Cloud Computing eine zentrale Rolle. In zukünftigen Ausgaben dieser Whitepaper-Reihe werden daher das Konzept der digitalen Souveränität und die Rolle von Cloud Computing (und die Rolle von Cloud-Anbietern) verbunden. Außerdem werden potenzielle Hebel zur Steigerung digitaler Souveränität im Cloud-Kontext (wie bspw. Multi-Cloud-Strategien sowie der Einsatz von Open-Source-Software und Verschlüsselungstechnologien) genauer beleuchtet.

Die Diskussion um digitale Souveränität in der Versicherungsbranche zeigt, dass das Thema von entscheidender Bedeutung ist, jedoch in der Praxis bislang nur indirekt und in Verbindung mit anderen strategischen Prioritäten adressiert wird. Weiter zu untersuchen ist, ob digitale Souveränität nur ein zufälliger Nebeneffekt, ein Mittel zum Zweck, eine differenzierende Strategie oder gar ein ökonomisch werthaltiges Unternehmensziel ist. Wenngleich im Rahmen dieses Whitepapers eine gewisse Tendenz gezeichnet wurde, bleiben diese Fragestellungen zunächst bewusst offen und Gegenstand individueller Analyse und Interpretation.

© GDV 2024

ÜBER DIE STUDIE UND DIE AUTOREN

Methodisches Vorgehen

Die dargestellten Daten beruhen auf einer qualitativen Studie von GDV und BELTIOS. Im Zeitraum Februar bis September 2024 wurden mehr als 30 Gespräche mit verschiedenen Versicherern, Technologie-Experten und Cloud-Anbietern geführt. Dabei wurden zunächst Entscheider aus der deutschen Versicherungsbranche (vorrangig Vertreter der IT-Organisationen) explorativ zu ihrer Haltung zum Konzept der digitalen Souveränität befragt. Die festgestellten Schwerpunktthemen, Problemstellungen und Interessen wurden in der Folge mit einer Reihe von Cloud-Anbietern diskutiert und in das vorliegende Whitepaper überführt. Dieses Whitepaper ist Teil einer Whitepaper-Reihe, deren Ziel es ist, ein Bewusstsein für digitale Souveränität zu schaffen und Versicherer dazu zu ermutigen, sich frühzeitig mit der Frage und Ausgestaltung ihrer eigenen digitalen Souveränität zu befassen.

Befragte Cloud-Anbieter: AWS, Microsoft, Google Cloud, IBM, OVHcloud, IONOS

Autoren

Patrik Maeyer
Leiter Betriebswirtschaft, Prozesse und IT
p.maeyer@gdv.de

Dr. Manuel Audi
Geschäftsführer BELTIOS & Leiter Business Consulting Insurance
manuel.audi@beltios.com

Florian Baltruschat
Referent Betriebswirtschaft, Prozesse und IT
f.baltruschat@gdv.de

Fabian Otto
Principal BELTIOS, Business Consulting Insurance
fabian.otto@beltios.com

GDV

Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) in Berlin ist die Dachorganisation der Versicherer in Deutschland. Gegenüber Parlament, Regierung und Öffentlichkeit – national wie auf europäischer Ebene – vertreten wir die Interessen der Branche.

BELTIOS

Die BELTIOS GmbH ist eine spezialisierte Unternehmensberatung für die Versicherungs- und Finanzdienstleistungsbranche und Teil des Beratungsnetzwerks msg advisors. Als kompetenter Ansprechpartner für Fach- und IT-Abteilungen sowie das Management unterstützt BELTIOS Unternehmen in Transformationsprozessen und beim Aufbau digitaler Ökosysteme. Die rund 80 Mitarbeiter vereinen fundierte versicherungsmathematische, -fachliche und -technische Expertise.

Mehr Informationen zu digitaler Souveränität finden Sie online:
https://advisors.msg.group/digitale-souveraenitaet/

© GDV 2024

GDV

Gesamtverband der Deutschen Versicherungswirtschaft e. V.
Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Tel.: +49 30 2020–5000, Fax: +49 30 2020–6000
www.gdv.de, berlin@gdv.de