Mein Zero-Trust Self-Assessment: Erreiche ich echte Datensouveränität?

buerokratie-automatisieren.de | Ein Informationsportal der J.v.G. technology GmbH
Mission: Bürokratische Prozesse durch Automatisierung und fundiertes Wissen vereinfachen.

Mein Zero-Trust Self-Assessment: Erreiche ich echte Datensouveränität?

Für wen ist dieses Dokument?
Für CISOs (Chief Information Security Officers, also die Verantwortlichen für Informationssicherheit), Datenschutzbeauftragte (DPOs) und technische Entscheider, die wissen wollen, wie souverän ihre Cloud-Architektur wirklich ist. Dieses Self-Assessment ersetzt oberflächliche Compliance-Checks durch eine ehrliche, strukturierte Bewertung. Sie beantworten Fragen, vergeben Punkte und erhalten am Ende ein klares Risikoprofil mit konkreten Handlungsfeldern. Das Ergebnis: Sie wissen genau, wo Ihre Architektur hält und wo sie bricht. Die zentrale Erkenntnis, die dieses Dokument antreibt: Echter Datenschutz entsteht nicht durch den Serverstandort, sondern durch eine Architektur, die Ihnen die technische Kontrolle über Ihre Daten gibt, unabhängig vom Anbieter.

So nutzen Sie dieses Dokument:
Drucken Sie es aus oder öffnen Sie es digital. Gehen Sie jede Frage für Ihre aktuelle Haupt-Cloud-Umgebung durch. Kreuzen Sie ehrlich an. Tragen Sie Ihre Punktzahl ein. Lesen Sie die Auswertung. Handeln Sie.

Sofort-Check: Stecken Sie in einer der 3 Souveränitäts-Fallen?

Bevor Sie das vollständige Assessment beginnen, prüfen Sie diese drei verbreiteten Fehleinschätzungen. Jedes „Ja" ist ein Warnsignal.

#	Die Falle	Prüffrage	Ja / Nein
1	**Der Standort-Mythos**	Verlassen Sie sich primär auf die Zusage Ihres Anbieters, dass die Daten in einem „deutschen" oder „europäischen" Rechenzentrum liegen, als Hauptargument für Ihre DSGVO-Konformität (Einhaltung der Datenschutz-Grundverordnung)?	☐ Ja / ☐ Nein
2	**Anbieterseitige Schlüssel**	Betrachten Sie die Standardverschlüsselung Ihres Cloud-Providers (z. B. „Encryption at Rest", also Verschlüsselung ruhender Daten auf dem Server) als ausreichenden Schutz gegen behördliche Zugriffe aus Drittstaaten?	☐ Ja / ☐ Nein
3	**Kein Exit-Plan**	Sind Ihre Daten und Abläufe so tief in proprietäre Dienste (herstellereigene, nicht standardisierte Systeme) eines einzigen Anbieters eingebettet, dass ein Wechsel unrealistisch erscheint?	☐ Ja / ☐ Nein

Auswertung Sofort-Check:

- **0 × Ja:** Gute Ausgangslage. Das vollständige Assessment wird zeigen, ob sie hält.
- **1 × Ja:** Es gibt eine relevante Schwachstelle. Lesen Sie weiter.
- **2–3 × Ja:** Ihre Souveränität basiert auf Annahmen, nicht auf Architektur. Dieses Dokument ist für Sie besonders wichtig.

Self-Assessment herunterladen

Teil 1: Datenverschlüsselung und Schlüsselkontrolle (max. 9 Punkte)

Hier liegt der Kern der Datensouveränität. Wer die kryptografischen Schlüssel kontrolliert, kontrolliert den Zugang zu den Daten. Nicht der Serverstandort entscheidet, sondern dieser Punkt.

Hintergrund: Der US CLOUD Act (Clarifying Lawful Overseas Use of Data Act, ein US-Bundesgesetz von 2018) verpflichtet US-Unternehmen, Daten auf behördliche Anordnung herauszugeben, auch wenn diese Daten auf Servern in der EU gespeichert sind. Der EuGH hat im Schrems-II-Urteil (Rechtssache C-311/18, 2020) das EU-US Privacy Shield für ungültig erklärt und klargestellt, dass rein vertragliche Schutzmaßnahmen gegen solche Zugriffe nicht ausreichen. Das European Data Protection Board (EDPB, der Europäische Datenschutzausschuss) hat in seinen Empfehlungen 01/2020 betont, dass „ergänzende technische Maßnahmen" nötig sind, bei denen der Anbieter keinen Zugriff auf die Klardaten hat.

Frage 1.1: Wo werden Ihre Daten verschlüsselt?

Option	Beschreibung	Punkte
☐ A	Nur auf den Servern des Anbieters (Standard-Verschlüsselung „at rest" und „in transit").	0
☐ B	Teilweise auf unseren Systemen, aber einige Dienste verarbeiten unverschlüsselte Daten.	1
☐ C	Vollständig auf unseren Systemen, bevor die Daten den Anbieter erreichen (Ende-zu-Ende-Verschlüsselung, also E2EE: Daten werden beim Absender verschlüsselt und erst beim Empfänger entschlüsselt).	3

Ihre Punkte Frage 1.1: ____

Frage 1.2: Wer kontrolliert die kryptografischen Schlüssel?

Option	Beschreibung	Punkte
☐ A	Der Cloud-Anbieter generiert und verwaltet alle Schlüssel.	0
☐ B	Wir nutzen BYOK (Bring Your Own Key: Wir liefern den Schlüssel, aber der Anbieter kann ihn im Betrieb nutzen).	1
☐ C	Wir nutzen HYOK (Hold Your Own Key: Wir behalten den Schlüssel, der Anbieter hat zu keinem Zeitpunkt Zugriff darauf) oder ein vergleichbares Verfahren mit voller Schlüsselhoheit.	3

Ihre Punkte Frage 1.2: ____

Frage 1.3: Kann der Support des Anbieters Ihre Daten im Klartext einsehen?

Option	Beschreibung	Punkte
☐ A	Ja, für Support- oder Wartungszwecke ist der Zugriff auf Klardaten möglich oder wahrscheinlich.	0
☐ B	Eingeschränkt, nur mit unserer expliziten Genehmigung und zeitlich begrenzt.	1
☐ C	Nein, der Support hat ausschließlich Zugriff auf verschlüsselte, für ihn unlesbare Datenblöcke.	3

Ihre Punkte Frage 1.3: ____

Zwischensumme Teil 1: ____ / 9

Was Ihr Ergebnis bedeutet:

- **7–9 Punkte:** Ihre Verschlüsselungsarchitektur ist stark. Die technische Kontrolle liegt bei Ihnen.
- **3–6 Punkte:** Teilweise Kontrolle. Die Lücken (insbesondere bei der Schlüsselverwaltung) sind potenzielle Einfallstore für Drittstaaten-Zugriffe.
- **0–2 Punkte:** Die Kontrolle über Ihre Daten liegt faktisch beim Anbieter. Vertragliche Zusagen sind hier Ihre einzige Schutzschicht, und das Schrems-II-Urteil hat gezeigt, dass diese allein nicht ausreichen.

Teil 2: Zugriffskontrolle und Anbieterunabhängigkeit (max. 9 Punkte)

Datensouveränität endet nicht bei der Verschlüsselung. Sie umfasst auch die Frage, ob Sie jederzeit handlungsfähig bleiben, also ob Sie den Anbieter wechseln, Daten abziehen oder Zugriffe nachweisbar unterbinden können.

Frage 2.1: Ist der Zugriff des Anbieters auf Ihre Daten technisch unterbunden?

Option	Beschreibung	Punkte
☐ A	Wir verlassen uns auf vertragliche und organisatorische Regelungen (z. B. SCCs, also Standardvertragsklauseln: von der EU-Kommission vorgegebene Vertragsmuster für Datentransfers in Drittstaaten).	0
☐ B	Wir haben zusätzliche organisatorische Maßnahmen implementiert (z. B. Zugriffsprotokollierung, Genehmigungsprozesse).	1
☐ C	Der Zugriff ist durch unsere clientseitige Verschlüsselung (Verschlüsselung auf dem eigenen Gerät oder Server, bevor Daten übertragen werden) technisch unmöglich, unabhängig von Verträgen.	3

Ihre Punkte Frage 2.1: ____

Frage 2.2: Wie hoch ist der Aufwand für einen vollständigen Anbieterwechsel?

Option	Beschreibung	Punkte
☐ A	Hoch bis sehr hoch. Wir nutzen viele proprietäre Dienste, ein Wechsel würde voraussichtlich mehr als 6 Monate dauern.	0
☐ B	Mittel. Einige Dienste sind portabel, aber Kernsysteme sind gebunden. Geschätzter Aufwand: 3–6 Monate.	1
☐ C	Gering. Unsere Daten liegen in portablen, standardisierten Formaten vor. Ein Wechsel ist in unter 3 Monaten realistisch.	3

Ihre Punkte Frage 2.2: ____

Ihre geschätzte Zeit für einen vollständigen Anbieterwechsel: _____ Monate

Proprietäre Dienste, die Sie am stärksten binden (bitte auflisten):

1. _____

2. _____

3. _____

Frage 2.3: Haben Sie eine dokumentierte und getestete Exit-Strategie?

Option	Beschreibung	Punkte
☐ A	Nein, es gibt keinen formalen Plan für einen Anbieterwechsel.	0
☐ B	Ein Plan existiert auf dem Papier, wurde aber nie praktisch getestet.	1
☐ C	Ja, es gibt einen dokumentierten, regelmäßig überprüften Exit-Plan inklusive Testmigrationen.	3

Ihre Punkte Frage 2.3: ____

Zwischensumme Teil 2: ____ / 9

Was Ihr Ergebnis bedeutet:

- **7–9 Punkte:** Sie sind handlungsfähig und unabhängig. Ein Anbieterwechsel ist eine Option, keine Krise.
- **3–6 Punkte:** Teilweise Unabhängigkeit. Identifizieren Sie die proprietären Dienste, die Sie am stärksten binden, und prüfen Sie offene Alternativen.
- **0–2 Punkte:** Hoher Vendor-Lock-in (starke Abhängigkeit von einem einzelnen Anbieter). Ihre Handlungsfähigkeit ist eingeschränkt. Im Fall einer regulatorischen Änderung oder eines Vertrauensbruchs stehen Sie unter Zeitdruck.

Gesamtauswertung: Ihr Souveränitätsprofil

Tragen Sie Ihre Zwischensummen ein:

Bereich	Ihre Punkte	Maximal
Teil 1: Verschlüsselung & Schlüsselkontrolle	____	9
Teil 2: Zugriffskontrolle & Unabhängigkeit	____	9
Gesamtpunktzahl	____	**18**

Ihre Risikostufe

15–18 Punkte: Architektonische Souveränität
Ihre Cloud-Architektur basiert auf technischer Kontrolle, nicht auf geografischen Versprechen oder reinen Vertragskonstrukten. Sie sind gut aufgestellt, auch wenn sich die regulatorische Lage erneut ändert (z. B. bei einer möglichen Aufhebung des EU-U.S. Data Privacy Framework, DPF). Empfehlung: Regelmäßige Überprüfung und Dokumentation beibehalten.

8–14 Punkte: Teilsouveränität mit Handlungsbedarf
Sie haben wichtige Grundlagen gelegt, aber es bestehen Kontrolllücken. Die häufigsten Schwachstellen in diesem Bereich: BYOK statt HYOK (der Anbieter kann den Schlüssel im Betrieb nutzen), fehlende Exit-Strategie oder ungetestete Notfallpläne. Empfehlung: Priorisieren Sie die Fragen, bei denen Sie Option A oder B gewählt haben. Jede davon ist ein konkreter Agendapunkt für Ihr nächstes Architektur-Review.

0–7 Punkte: Souveränität auf dem Papier
Ihre Datensouveränität beruht überwiegend auf Vertrauen, Verträgen und dem Standortversprechen Ihres Anbieters. Das ist die Position, die das Schrems-II-Urteil des EuGH (2020) als unzureichend identifiziert hat. Sie sind den Risiken des US CLOUD Act und künftiger regulatorischer Umbrüche direkt ausgesetzt. Empfehlung: Beginnen Sie mit der Schlüsselhoheit (Frage 1.2). Sie ist der wirksamste einzelne Hebel auf dem Weg zu echter Kontrolle.

Entscheidungsmatrix: Wo anfangen?

Wenn Ihre Schwäche hier liegt …	… dann ist Ihr nächster Schritt:
Frage 1.1 oder 1.2 (Verschlüsselung/Schlüssel)	Evaluierung einer HYOK- oder clientseitigen Verschlüsselungslösung. Dies ist der wirksamste Einzelschritt.
Frage 1.3 (Support-Zugriff)	Prüfung, ob Ihr Anbieter einen „Confidential Computing"-Modus (Datenverarbeitung in geschützten Speicherbereichen, auf die auch der Betreiber keinen Zugriff hat) oder vergleichbare Modelle anbietet.
Frage 2.1 (Technische vs. vertragliche Kontrolle)	Ergänzung der SCCs durch die in den EDPB-Empfehlungen 01/2020 geforderten technischen Maßnahmen (insbesondere Verschlüsselung ohne Anbieterzugriff auf den Schlüssel).
Frage 2.2 oder 2.3 (Lock-in/Exit)	Erstellung eines dokumentierten Exit-Plans. Identifizierung aller proprietären Abhängigkeiten und Prüfung portabler Alternativen.

Ein reales Szenario: Die behördliche Datenanfrage

Dieses Szenario zeigt den konkreten Unterschied zwischen den beiden Architekturen.

Szenario A — Ohne Zero-Trust-Architektur (Architekturprinzip „Vertraue niemandem, überprüfe alles": Jeder Zugriff wird verifiziert, kein Nutzer oder System erhält automatisch Vertrauen):
Eine US-Behörde stellt eine Anfrage nach dem CLOUD Act an Ihren US-amerikanischen Cloud-Provider. Der Provider ist gesetzlich zur Kooperation verpflichtet. Da er die Verschlüsselungsschlüssel verwaltet, entschlüsselt er Ihre Daten und übergibt sie im Klartext. Sie erfahren davon unter Umständen nie, da der CLOUD Act keine Benachrichtigungspflicht gegenüber dem Dateninhaber vorsieht.

Szenario B — Mit Zero-Trust-Architektur und Schlüsselhoheit:
Dieselbe Anfrage trifft ein. Der Provider ist weiterhin zur Kooperation verpflichtet. Er kann jedoch nur verschlüsselte, für die Behörde unlesbare Datenblöcke übergeben. Er besitzt die Schlüssel nicht. Die Kontrolle über die Entschlüsselung liegt ausschließlich bei Ihnen. Der technische Schutz wirkt unabhängig davon, in welchem Land der Server steht.

Was die meisten unterschätzen:
Viele Organisationen gehen davon aus, dass der Wechsel zu einem europäischen Cloud-Anbieter dieses Problem löst. Das reduziert zwar das Risiko eines CLOUD-Act-Zugriffs, schafft aber keine architektonische Souveränität. Auch ein europäischer Anbieter, der Ihre Schlüssel verwaltet, hat technisch die Möglichkeit, Ihre Daten im Klartext einzusehen. Und auch europäische Jurisdiktionen kennen behördliche Datenzugriffsrechte (z. B. unter nationalen Polizei- und Sicherheitsgesetzen). Der entscheidende Schutz ist nicht die Nationalität des Anbieters, sondern Ihre Schlüsselhoheit.

Warum das für Ihre Bürokratie-Automatisierung entscheidend ist

Wenn Sie bürokratische Prozesse automatisieren und in die Cloud verlagern, verarbeiten Sie dort zwangsläufig sensible Daten: Personalakten, Steuerunterlagen, Verträge, Kundendaten. Jede Automatisierung, die auf einem Fundament ohne technische Datensouveränität steht, birgt ein regulatorisches Risiko, das den gesamten Effizienzgewinn zunichtemachen kann. Ein Bußgeldbescheid, eine Untersagungsverfügung oder ein erzwungener Anbieterwechsel unter Zeitdruck kosten mehr als jede Automatisierung einspart. Echte Datensouveränität durch eine Zero-Trust-Architektur ist daher keine Zusatzoption, sondern die Voraussetzung dafür, dass Ihre automatisierten Prozesse dauerhaft rechtssicher und zukunftsfähig bleiben.

Zusammenfassung und Ihre nächsten Schritte

Sie haben jetzt eine fundierte, ehrliche Einschätzung Ihrer Datensouveränität. Die Fragen, bei denen Sie Option A gewählt haben, sind Ihre dringendsten Handlungsfelder. Die Fragen mit Option B zeigen Bereiche, die verbessert werden können und sollten.

Ihr Ergebnis ist Ihr Werkzeug. Nutzen Sie dieses Assessment als Agenda für Ihr nächstes Architektur-Meeting oder als Gesprächsgrundlage mit Ihrer Geschäftsleitung.

Schritt 1 — Vertiefen Sie Ihr Wissen:
Lesen Sie den vollständigen Leitfaden „Nach Schrems II: Warum ‚Deutsche Server' eine Scheinlösung sind und nur eine Zero-Trust-Architektur wirklich schützt" auf buerokratie-automatisieren.de, um die technischen und rechtlichen Hintergründe im Detail zu verstehen.

Schritt 2 — Holen Sie spezialisierte Beratung ein:
Wenn Ihre Gesamtpunktzahl unter 14 liegt, ziehen Sie einen auf Datenschutzrecht und Cloud-Sicherheit spezialisierten Berater oder eine Kanzlei hinzu. Bringen Sie dieses ausgefüllte Assessment mit — es gibt dem Gespräch sofort eine konkrete Grundlage.

Speichern oder drucken Sie dieses Dokument. Es ist Ihre Landkarte von der geografischen Hoffnung zur architektonischen Gewissheit.

buerokratie-automatisieren.de

Ein Informationsportal der J.v.G. technology GmbH

Bürokratische Prozesse durch Automatisierung und fundiertes Wissen vereinfachen.

Konzeption und AI-Visibility-Architektur: JvGLabs — AI visibility architecture

Self-Assessment herunterladen