

Checkliste: Souveränitätsbewertung Cloud- und KI-Stack

20 Fragen, eine Stunde, eine erste Selbsteinschätzung. Das Ergebnis ist eine Indikation, keine abschließende Bewertung Ihrer Souveränitätslage. Bewerten Sie jede Frage mit 2 Punkten (ja, belegbar), 1 Punkt (teilweise oder ungeprüft) oder 0 Punkten (nein oder unbekannt). Maximal 40 Punkte.

A · Datenlokation und Transfers

Frage	2	1	0
Wir wissen für jedes produktive System, in welcher Region Daten gespeichert und verarbeitet werden.			
Drittlandübermittlungen sind je System identifiziert und mit gültigen Garantien unterlegt (aktive DPF-Zertifizierung des Anbieters oder SCC plus TIA).			
Transfer Impact Assessments existieren und sind jünger als 24 Monate.			
Support- und Fernwartungszugriffe aus Drittländern sind bekannt und vertraglich geregelt.			

B · Vertrag und Exit (Data Act)

Frage	2	1	0
Unsere Cloud-Verträge enthalten konkrete Regelungen zu Datenexport, Formaten und Unterstützungspflichten beim Wechsel.			
Für die zwei kritischsten Abhängigkeiten existiert ein dokumentiertes, mit Aufwand und Dauer beziffertes Exit-Szenario.			
Wechselentgelte und Kündigungsfristen sind erfasst und gegen die Vorgaben des Data Act geprüft.			
Ein vollständiges Register aller Cloud- und SaaS-Dienstleister existiert und wird gepflegt.			



C · Zugriff und Kontrolle

Frage	2	1	0
Verschlüsselung ruhender und übertragener Daten ist Standard; die Schlüsselhoheit ist bekannt und bewusst gewählt.			
Administrative Zugriffe des Anbieters auf unsere Daten sind transparent, protokolliert und auditierbar.			
Die Rechtslage zu behördlichen Zugriffen aus Drittstaaten auf unsere Anbieter ist bewertet und dokumentiert.			
Identitäts- und Berechtigungsmanagement liegt in unserer Hoheit, nicht allein beim Anbieter.			

D · KI-spezifisch

Frage	2	1	0
Alle KI-Systeme und eingebauten KI-Funktionen sind inventarisiert und im Verarbeitungsverzeichnis abgebildet.			
Für jedes KI-Tool ist geregelt und geprüft, ob Eingaben zum Training des Anbieters verwendet werden.			
Der Verarbeitungsort der KI-Modelle (Region, Anbieter, Subprozessoren) ist je System bekannt.			
Freigegebene und nicht freigegebene KI-Tools sind für Beschäftigte eindeutig unterscheidbar kommuniziert.			

E · Meldefähigkeit

Frage	2	1	0
Ein Prozess stellt sicher, dass Datenpannen in fremdbetriebenen Systemen uns rechtzeitig bekannt werden (Vertragspflicht des Anbieters).			
Die 72-Stunden-Meldung nach Art. 33 DSGVO ist als Prozess mit Rollen und Vorlagen etabliert und getestet.			
Zuständigkeiten zwischen DSB, IT-Leitung und Geschäftsführung im Vorfall sind schriftlich geregelt.			
Meldewege weiterer Regime (NIS2, ggf. DORA, CRA seit 11.09.2026) sind geprüft und eingerichtet.			

Auswertung

32 bis 40 Punkte

Die Indikation spricht für eine solide Aufstellung. Eine jährliche Überprüfung erscheint ausreichend; Fokus auf Vertragsanpassungen bei Verlängerungen.

20 bis 31 Punkte

Die Indikation deutet auf strukturierten Handlungsbedarf. Die Lücken sind bekannt oder mit dieser Liste jetzt sichtbar; ein priorisierter Maßnahmenplan kann sie erfahrungsgemäß in 6 bis 12 Monaten schließen.

unter 20 Punkte

Die Indikation deutet auf kritische Abhängigkeiten. Sinnvoller Startpunkt ist das Inventar (Block A und D), alles Weitere baut darauf auf.

Nächster Schritt

Im Erstgespräch gehen wir Ihre Bewertung gemeinsam durch und priorisieren die drei wirksamsten Maßnahmen für Ihren Stack.

Kontakt: governance-first.de · Questax Systems GmbH, Heidelberg

Wichtiger Hinweis zur Nutzung dieses Dokuments. Dieses Dokument dient der ersten Orientierung und als initiale Vorabprüfung. Es stellt weder eine abschließende Bewertung noch eine Rechtsberatung im Sinne des Rechtsdienstleistungsgesetzes (RDG) dar und ersetzt keine einzelfallbezogene Prüfung durch qualifizierte Fachanwälte oder zertifizierte Compliance-Expertinnen und -Experten. Gesetzliche Fristen und Pflichten sind nach bestem Wissen zum angegebenen Stand wiedergegeben; maßgeblich sind stets die amtlichen Rechtstexte und die aktuelle Verwaltungspraxis der zuständigen Aufsichtsbehörden. Trotz sorgfältiger Erstellung wird keine Gewähr für Vollständigkeit, Richtigkeit und Aktualität übernommen. Eine Haftung der Questax Systems GmbH für Entscheidungen, die allein auf Grundlage dieses Dokuments getroffen werden, ist ausgeschlossen.