skaylink
A Vodafone company

AWS Sovereignty Assessment

Define Sovereignty
Before You Architect It

Vielfältige regulatorische Vorgaben und neue Cloud-Modelle wie die AWS European Sovereign Cloud erhöhen die Ansprüche an digitale Souveränität. Mit dem Skaylink AWS Sovereignty Assessment identifizieren Sie Anforderungen, bewerten Risiken und entwickeln eine fundierte Sovereignty-Strategie für Ihre AWS-Umgebung.

Warum ein Sovereignty Assessment?

Viele Organisationen stehen vor denselben Fragen:

- Welche Workloads sind von regulatorischen Anforderungen betroffen?
- Welche Daten müssen in der EU oder sogar in Deutschland verbleiben?
- Welche Anforderungen sind regulatorisch verpflichtend und welche beruhen auf internen Unternehmensrichtlinien?
- Welche AWS-Infrastruktur erfüllt unsere Anforderungen?

Ohne eine klare Anforderungsbasis drohen entweder Überregulierung und unnötige Kosten oder Compliance-Risiken durch unzureichende Schutzmaßnahmen.

Was beinhaltet das Assessment?

Expert Review & Beratung

Bewertung durch AWS- und Sovereignty-Expert*innen

Executive Report & Roadmap

Priorisierte Handlungsempfehlungen und Zielarchitektur für Ihre AWS-Umgebung

Persönliche Beratung mit Sovereignty Scan

Analyse der AWS-Landschaft hinsichtlich Datenresidenz, Governance, Verschlüsselung und Compliance

Ergebnis des Assessments

- ✓ Sovereignty-Reifegradbewertung
- ✓ Risiko- und Gap-Analyse
- ✓ Architektur- und Infrastrukturempfehlungen
- ✓ Priorisierte Maßnahmen
- ✓ Managementtauglicher Ergebnisbericht
- ✓ Readiness Check für die AWS European Sovereign Cloud

skaylink
A Vodafone company

AWS Sovereignty Assessment

Define Sovereignty
Before You Architect It

Unser 7-Domain Sovereignty Framework

Das Assessment basiert auf einem strukturierten Framework, das die drei zentralen Säulen digitaler Souveränität betrachtet: Compliance, Kontrolle und Kontinuität.

Kontext verstehen

D1 – Businessziele & Anforderungen
- Strategische Treiber
- Kritische Geschäftsprozesse
- Nicht verhandelbare Anforderungen
- Stakeholder und Verantwortlichkeiten

D2 – Regulatorik & Jurisdiktion
- Branchenspezifische Vorgaben
- Compliance- und Rechtsanforderungen
- Jurisdiktion und Datenhoheit

D3 – Datenklassifizierung
- Dateninventar
- Kritische Datenbestände
- KI- und Trainingsdaten
- Daten-Governance

Die Sovereignty-Säulen bewerten

D4 – Data Sovereignty & Protection
- Datenstandorte
- Datenübertragungen
- Verschlüsselung
- Schlüsselmanagement

D5 – Resilience & Independence
- Disaster Recovery
- Provider-Abhängigkeiten
- Exit-Strategien
- Betriebsfähigkeit unter regulatorischen Einschränkungen

D6 – Operational Sovereignty & Access
- Zugriffsmodelle
- Rollen und Verantwortlichkeiten
- Jurisdiktionsanforderungen
- Betriebs- und Supportmodelle

Nachhaltige Governance

D7 – Continuous Assurance
- Compliance-Monitoring
- Auditfähigkeit
- Evidenzmanagement
- Drift Detection
- KPIs und kontinuierliche Verbesserung

Haben Sie noch Fragen?

Wir helfen Ihnen gerne weiter:

awspartner@skaylink.com