

SOVEREIGN CLOUD COMPASS · MARKTANALYSE

European Cloud Sovereignty Report 2026.

Evidenzbasierte Analyse von 17 Sovereign-Cloud-Angeboten im europäischen Markt, gemessen an 31 Kriterien auf sechs Souveränitätsachsen, vollständig auf das EU Cloud Sovereignty Framework abgebildet.

17

ANBIETER

31

KRITERIEN

6

ACHSEN

8

EU-CSF-ZIELE

334

QUELLEN

HERAUSGEBER

Jörn Petereit
IT Capital Partners GmbH, Hamburg

ERSCHEINUNGSDATUM

Mai 2026
sovereigncloudcompass.de

INHALTSVERZEICHNIS

Inhalt.

Sieben Teile, ein Anhang. Jeder Teil ist eigenständig lesbar; der Compass auf sovereigncloudcompass.de hält die Detailbewertungen mit Quellenverweis.

EXECUTIVE SUMMARY

–	Zusammenfassung	04
---	-----------------	----

TEIL I

01	Marktlage und regulatorisches Umfeld	06
	Souveränitätsdebatte im Frühjahr 2026	06
	Regulatorische Landschaft (CSF, BSI C5, SecNumCloud)	07
	Sovereignty Washing: Das Kernproblem des Marktes	08

TEIL II

02	Methodik	10
	Scope-Kategorien, Achsen, EU-CSF-Referenz, Grundsätze	10

TEIL III

03	Marktübergreifende Befunde	13
	Befund 1 – Kein Gesamtsieger	13
	Befund 2 – Kryptografie als Sorgenkind	15
	Befund 3 – Die Transparenz-Lücke	16
	Befund 4 – Dienstportfolio vs. Souveränität	17
	Befund 5 – Compliance-Dynamik	18
	Befund 6 – Die ökonomische Dimension	19

TEIL IV

04	Anbieterprofile (17)	20
----	----------------------	----

TEIL V

05	Sektorspezifische Anwendungsfälle	37
	Verwaltung · KRITIS · Finanzsektor · Gesundheitswesen	37

TEIL VI

06	EU-CSF-Referenzsicht	41
----	----------------------	----

TEIL VII

07	Ausblick und offene Fragen	43
----	----------------------------	----

ANHANG

A	Kriterienkatalog (31 Kriterien)	45
B	Rechtliche Hinweise und Nutzungsbedingungen	47
–	Impressum	48

Wer Souveränität nicht messen kann, entscheidet nicht.

Er folgt dem überzeugendsten Narrativ. Der European Cloud Sovereignty Report 2026 ist die erste unabhängige, evidenzbasierte Marktanalyse europäischer Sovereign-Cloud-Angebote, vollständig auf das EU Cloud Sovereignty Framework abgebildet.

17 / 31

ANBIETER / KRITERIEN

72,8

HÖCHSTER EU-SCORE
(T CLOUD PUBLIC)

2,09_{/5}

MARKTDURCHSCHNITT KRYPTOGRAPHIE

KERNBEFUNDE

Der Report bewertet 17 Anbieter anhand 31 Kriterien auf sechs Souveränitätsachsen, gestützt auf 334 öffentlich verfügbare Quellen. Die Methodik ist konservativ: N/A wird als 0 gewertet, fehlende Nachweise als Risiko behandelt.

Die Analyse zeigt ein differenziertes Bild eines Marktes, in dem Souveränitätsversprechen und operative Realität oft erheblich auseinanderklaffen.

Kein Gesamtsieger.

Kein Anbieter führt in allen sechs Souveränitätsachsen gleichzeitig. T Cloud Public erreicht als einziger in keiner Achse unter 3,5/5 und erzielt mit 72,8/100 den höchsten EU-Souveränitätsscore. Unter den EU-nativen Anbietern folgen SysEleven OpenStack Cloud (68,8) und STACKIT (67,3); AWS European Sovereign Cloud erreicht zwar 71,4, bleibt aber bei Recht & Jurisdiktion auf 2,1 gedeckelt.

Sovereignty Washing auf beiden Seiten des Atlantiks.

US-Hyperscaler vermarkten EU-Tochtergesellschaften als souverän, bleiben aber bei Recht & Jurisdiktion strukturell gedeckelt: AWS European Sovereign Cloud erreicht 2,1/5, Microsoft Sovereign Cloud 0,9/5, Oracle EU 2,1/5. Gleichzeitig betreiben europäische Anbieter die umgekehrte Variante: Sie vermarkten EU-Eigentümerschaft als Alleinstellungsmerkmal, erreichen aber bei Confidential Computing und technischen Schutzmaßnahmen teils nur 0 oder 1 von 5 Punkten.

Kryptografie & Schlüsselkontrolle ist das Sorgenkind des Marktes.

Mit einem Marktdurchschnitt von 2,09/5 ist dies die schwächste aller sechs Achsen. Operator Access Exclusion liegt bei 1,94/5, EU-Stammzertifizierungsstellen bei 1,59/5 und unabhängige Advisory Boards bei 0,47/5. Hardwaregestützte Workload-Isolation über AMD SEV-SNP oder Intel TDX ist weit entfernt vom Marktstandard.

Das Portfolio-Souveränitäts-Dilemma.

Die breitesten Dienstportfolios (AWS, Oracle, Microsoft je 100% der 33 bewerteten Dienste) gehören den Anbietern mit den niedrigsten Jurisdiktionswerten. EU-native IaaS-Anbieter bieten hohe Souveränität, aber schmale Portfolios (noris 12%, Hetzner 27%). Für Enterprise-Workloads mit IAM, Container-Orchestrierung und Observability ist dies ein realer Engpass.

Compliance-Dynamik erfordert kontinuierliche Aktualisierung.

Allein zwischen Februar und März 2026 haben AWS European Sovereign Cloud (BSI C5 Typ 1 für 69 Services, Score 2→4), STACKIT (C5 Typ 2 bestätigt, Score 3→5) und T Cloud Public signifikante Compliance-Upgrades erzielt. Dieser Report bildet den Stand März 2026 ab; die Webapp wird laufend aktualisiert.

TEIL I

Marktlage und regulatorisches Umfeld.

Cloud-Souveränität hat sich von einem Nischenthema für Datenschutzbeauftragte zu einem zentralen Beschaffungskriterium für regulierte Organisationen entwickelt. Was sich geändert hat, ist die Intensität.

01.1

Die Souveränitätsdebatte im Frühjahr 2026.

Die Treiber sind bekannt: DSGVO-Enforcement, Schrems-II-Nachwirkungen, IT-Sicherheitsgesetz 2.0, NIS2 (umgesetzt seit Oktober 2024), DORA (anwendbar seit Januar 2025), Cyber Resilience Act (seit Dezember 2024), sektorspezifische Regulierung in Finanz- und Gesundheitswesen, und nicht zuletzt die geopolitische Neubewertung technologischer Abhängigkeiten, die seit 2022 wirkt und mit der zweiten Trump-Administration noch einmal an Schärfe gewonnen hat.

Was sich geändert hat, ist die Intensität: Nahezu jeder große Cloud-Anbieter vermarktet inzwischen ein „souveränes“ Angebot. AWS hat die European Sovereign Cloud am 15. Januar 2026 in der Region Brandenburg in den GA-Status überführt, Microsoft betreibt eine EU Data Boundary, Oracle hat eine dedizierte EU Sovereign Cloud aufgesetzt. Auf europäischer Seite konkurrieren Dutzende Anbieter mit unterschiedlichsten Souveränitätsversprechen um regulierte Workloads.

Die zentrale Herausforderung für IT-Entscheider ist damit nicht mehr die Verfügbarkeit souveräner Angebote, sondern deren Vergleichbarkeit. Wenn jeder Anbieter „souverän“ für sich beansprucht, mit höchst unterschiedlicher Substanz hinter dem Label, wird ein evidenzbasierter Bewertungsrahmen zur Notwendigkeit.

BEGRIFFSABGRENZUNG

Souveränität als selbstbestimmte Risikoentscheidung.

Eine Grenze des Bewertungsrahmens ist explizit zu nennen: Der Compass misst die Souveränitätseigenschaften einzelner Anbieter, nicht die Souveränität einer IT-Strategie. Souveränität endet nicht bei struktureller Unabhängigkeit, sondern umfasst die selbstbestimmte Risikoentscheidung. Eine bewusst gewählte Multi-Cloud- oder Hybrid-Architektur mit BYOK, dokumentiertem Exit-Pfad und regelmäßigen Disaster-Recovery-Tests kann ein legitimer souveräner Weg sein, auch wenn einzelne Komponenten nicht-souverän sind.

Regulatorische Landschaft.

EU Cloud Sovereignty Framework (CSF v1.2.1)

Acht Souveränitätsziele (SOV-1 bis SOV-8) und vier SEAL-Stufen als Reifegradmodell. Die derzeit substanziellste europäische Referenz. Der Compass bildet alle 31 Kriterien vollständig auf die acht CSF-Ziele ab und berechnet eine EU-Referenzsicht mit Souveränitätsscore (0–100) und SEAL-Näherung (0–4).

BSI C5 und IT-Grundschutz

Zentrales Prüfinstrument in Deutschland. IT-Grundschutz bleibt mit einem Marktdurchschnitt von 1,24/5 eines der schwächsten Kriterien, ein Indikator dafür, dass das BSI-Rahmenwerk für viele Anbieter noch kein Standardrepertoire ist.

SecNumCloud (Frankreich)

Eigener Zertifizierungspfad mit expliziten Eigentümerschafts- und Jurisdiktionsanforderungen. Marktdurchschnitt 0,76/5, ein Differenzierungsmerkmal, kein Standard.

01.2 · DAS KERNPROBLEM DES MARKTES

Sovereignty Washing.

Die systematische Überbetonung eines einzelnen Souveränitätsaspekts bei gleichzeitiger Vernachlässigung anderer, gleichwertiger Dimensionen. Das Phänomen tritt in zwei Varianten auf, und keine davon ist auf eine Seite des Atlantiks beschränkt.

VARIANTE A

US-HYPERSCALER

Die GmbH-Kulisse.

EU-Tochtergesellschaften und EU-Bürger im Advisory Board überdecken die rechtliche Zugriffsproblematik. Die technischen Guardrails sind teils belastbarer als bei manchem europäischen Wettbewerber, doch die juristische Konstruktion ändert nichts an der extraterritorialen Reichweite.

ANBIETER	EIGENTÜMER-SCHAFT	OPERATOR ACCESS
AWS European Sovereign Cloud	1	4
Microsoft Sovereign Cloud	0	3
Oracle EU Sovereign Cloud	1	4

Werte auf Fünferskala (0–5). Die Asymmetrie zwischen rechtlichem und technischem Schutz macht die Konstruktion sichtbar.

VARIANTE B

EU-NATIVE ANBIETER

Die EU-Flagge als Schutzschild.

EU-Eigentümerschaft wird als Alleinstellungsmerkmal in den Vordergrund gestellt. Das Argument ist nicht falsch, aber unvollständig: Die Lücke zwischen rechtlichem und technischem Schutz beträgt bei einigen Anbietern mehr als drei Stufen auf der Fünferskala – und bleibt im Marketing meist unerwähnt.

ANBIETER	RECHT & JURISD.	CONF. COMPUTING
Hetzner	4,1	0
Scaleway	4,1	0
Infomaniak	3,5	0

Werte auf Fünferskala (0–5). Die EU-Flagge ersetzt keine hardwaregestützte Workload-Isolation.

Beide Varianten bedienen sich derselben Mechanik: Ein leicht messbarer und gut vermarktbarer Aspekt wird zum Synonym für Souveränität erklärt, während andere Achsen unter dem Radar bleiben. Der Unterschied liegt nur in der Richtung, in die kaschiert wird.

“Wer Souveränität nicht messen kann, entscheidet nicht, er folgt dem überzeugendsten Narrativ.”

TEIL II

Methodik.

17 Anbieter. 31 Kriterien. 334 Quellen. Sechs Souveränitätsachsen, vollständig auf das EU Cloud Sovereignty Framework abgebildet.

Scope-Kategorien.

Die bewerteten Anbieter unterscheiden sich fundamental in der Tiefe ihres Dienstangebots. Tiefe und Breite sind dabei zwei unabhängige Dimensionen.

KATEGORIE	BESCHREIBUNG	ANBIETER
IAAS	Compute, Storage, Netzwerk. Grundlegende Cloud-Infrastruktur.	IONOS Cloud, UpCloud, Hetzner Cloud
IAAS+	IaaS + Managed Services (K8s, DB, Backup).	OVHcloud, T Cloud Public, pluscloud open, Exoscale, noris, SysEleven, Infomaniak
CLOUD SUITE	IaaS + PaaS (Container, Serverless, KI/ML, DB).	AWS ESC, STACKIT, Oracle EU, Scaleway, Cloud Temple
FULL STACK	IaaS + PaaS + SaaS (Office-Suite-Tiefe).	Delos Cloud, Microsoft Sovereign Cloud

Sechs Souveränitätsachsen.

ACHSE	PRÜFGEGENSTAND
Datenresidenz	Verarbeitung in EU/EWR.
Operationale Souveränität	Betrieb durch EU-Akteure.
Recht & Jurisdiktion	Eigentümer, FISA-702, EU-Recht.

Bewertungsskala 0–5.

- 0 Nicht erfüllt, keine belastbare Evidenz.
- 1 Angekündigt oder behauptet, ohne Nachweis.
- 2 Teilerfüllung, signifikante Lücken.
- 3 Erfüllung im Standardumfang.
- 4 Substantielle Erfüllung, breit dokumentiert.
- 5 Vollständige Erfüllung, unabhängig nachweisbar.

ACHSE	PRÜFGEGENSTAND
Kryptografie	Schlüsselhoheit, Operator-Ausschluss.
Transparenz	Prüfberichte, kontinuierliche Verifikation.
Portabilität	Offene Standards, kein Lock-in.

Methodische Grundsätze.

- Evidenzbasiert. Mindestens eine öffentliche Quelle pro Bewertung.
- Konservativ. N/A wird als 0 im EU-Score gewertet.
- Konsistent. Alle Anbieter, dieselben Kriterien.
- Transparent. Gewichtung offengelegt und anpassbar.
- Vendorneutral. Eigenfinanziert, frei verfügbar.

EINORDNUNG

Gartner Magic Quadrant und ISG Provider Lens bewerten Cloud-Anbieter primär nach technischer Reife und Marktpräsenz, ENISA-Reports liefern regulatorische Einordnungen ohne anbieterspezifische Scores. Der Sovereign Cloud Compass füllt die Lücke zwischen diesen Perspektiven, vollständig EU-CSF-aligniert. Bewusst komplementär, nicht konkurrierend.

BEFUND 01 · VON 06

Kein Anbieter führt in allen sechs Achsen.

T Cloud Public erreicht als einziger in keiner Achse unter 3,5/5. SysEleven und noris zeigen, dass starke Governance und solide Technik gleichzeitig möglich sind. Hyperscaler liefern bei Portabilität überdurchschnittliche Werte, bleiben bei Recht & Jurisdiktion strukturell gedeckelt.

SKALENLEGENDE

5

Vollständig

4

Substantiell

3

Standard

2

Teilerfüllung

<2

Schwach

ÜBERSICHT: 17 ANBIETER, SORTIERT NACH EU-SCORE

SECHS SOUVERÄNITÄTSACHSEN · SKALA 0-5 · EU-SCORE 0-100 · SEAL 0-3

ANBIETER	EU- SCORE	SEAL	DATEN	OPERATIV	RECHT	KRYPTO	TRANSP.	PORTAB.	ABDECKUNG
T Cloud Public	72,8	2	4,2	3,6	4,3	3,5	3,6	3,6	97%
AWS European Sovereign Cloud	71,4	1	3,8	3,9	2,1	3,0	3,2	4,6	100%
SysEleven OpenStack Cloud	68,8	1	3,9	3,3	4,3	2,5	3,9	3,8	36%
STACKIT	67,3	1	3,2	3,9	4,1	2,0	3,4	3,2	70%
noris Sovereign Cloud	66,0	1	3,9	3,2	4,3	2,5	2,9	3,4	12%
Cloud Temple Trusted Cloud	65,1	0	4,4	3,5	4,1	2,5	2,4	3,2	55%
OVHcloud Public Cloud	64,8	1	2,9	3,1	3,8	2,0	2,8	3,4	52%
Oracle EU Sovereign Cloud	63,4	1	4,0	3,9	2,1	2,0	1,8	3,5	100%
Scaleway	63,3	1	3,0	2,3	4,1	1,5	2,0	3,6	76%
Delos Cloud	61,6	1	3,9	3,4	4,0	2,5	1,9	2,9	91%
IONOS Cloud	60,5	1	2,9	2,3	3,8	1,5	2,9	3,8	64%
Infomaniak Public Cloud	58,5	0	3,1	2,7	3,5	1,5	1,6	3,1	42%
Hetzner Cloud	57,4	1	3,0	2,2	4,1	1,5	2,9	2,7	27%
UpCloud	56,2	0	3,0	3,1	4,1	1,5	1,4	3,3	39%
pluscloud open	52,0	0	3,2	3,0	2,7	2,0	2,9	3,3	24%
Exoscale	50,9	0	3,0	2,1	2,9	1,5	2,7	3,2	39%
Microsoft Sovereign Cloud	49,2	0	3,2	2,7	0,9	2,0	3,6	4,5	100%

Achsen: Daten = Datenresidenz · Operativ = Operative Souveränität · Recht = Recht & Jurisdiktion · Krypto = Kryptographie · Transp. = Transparenz · Portab. = Portabilität.
Sortiert nach EU-Souveränitätsscore (0-100), Achsenwerte 0-5. SPOT rev20, März 2026.

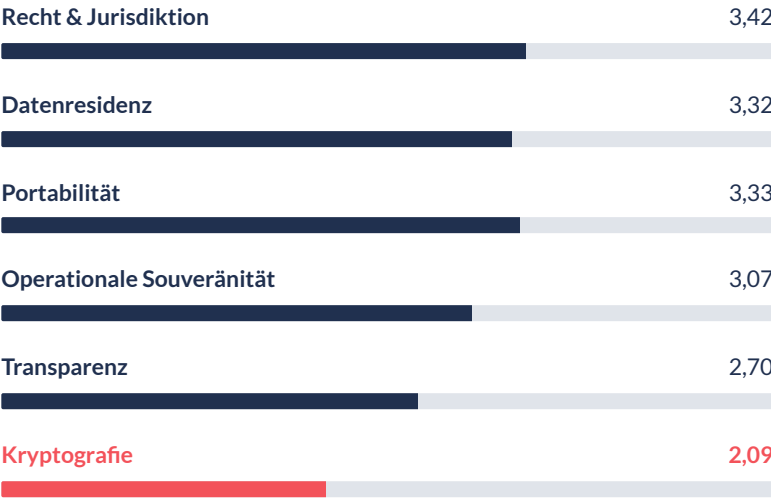
BEFUND 02 · VON 06

Kryptografie als Sorgenkind.

Mit 2,09/5 weist die Achse Kryptografie & Schlüsselkontrolle den niedrigsten Marktdurchschnitt aller sechs Achsen auf. Nur T Cloud Public erreicht mehr als 3,0 Punkte.

Hardwaregestützte Workload-Isolation über AMD SEV-SNP oder Intel TDX ist weit entfernt vom Marktstandard. Ein Anbieter kann vollständig in EU-Hand sein und trotzdem keine dokumentierte Operator-Exclusion vorweisen.

ACHSEN-MARKTDURCHSCHNITT



Marktdurchschnitt über 17 Anbieter, Skala 0–5.

Drei zentrale Schwächen.

1,94^{/5}

Operator Access Exclusion.

AWS ESC (Nitro), STACKIT (Confidential Server) und Oracle EU (OCI Confidential VMs) erreichen mit 4/5 die höchsten Werte. Die Mehrheit der EU-nativen Anbieter bietet keine dokumentierte hardwaregestützte Exclusion.

1,59^{/5}

EU Root CA / Trust Services.

Die meisten Anbieter verwenden TLS-Zertifikate globaler Certificate Authorities. Nur wenige nutzen eIDAS-qualifizierte EU Trust Service Provider. Delos Cloud setzt über D-Trust (Bundesdruckerei) einen Akzent.

0,47^{/5}

Unabhängiges Advisory Board.

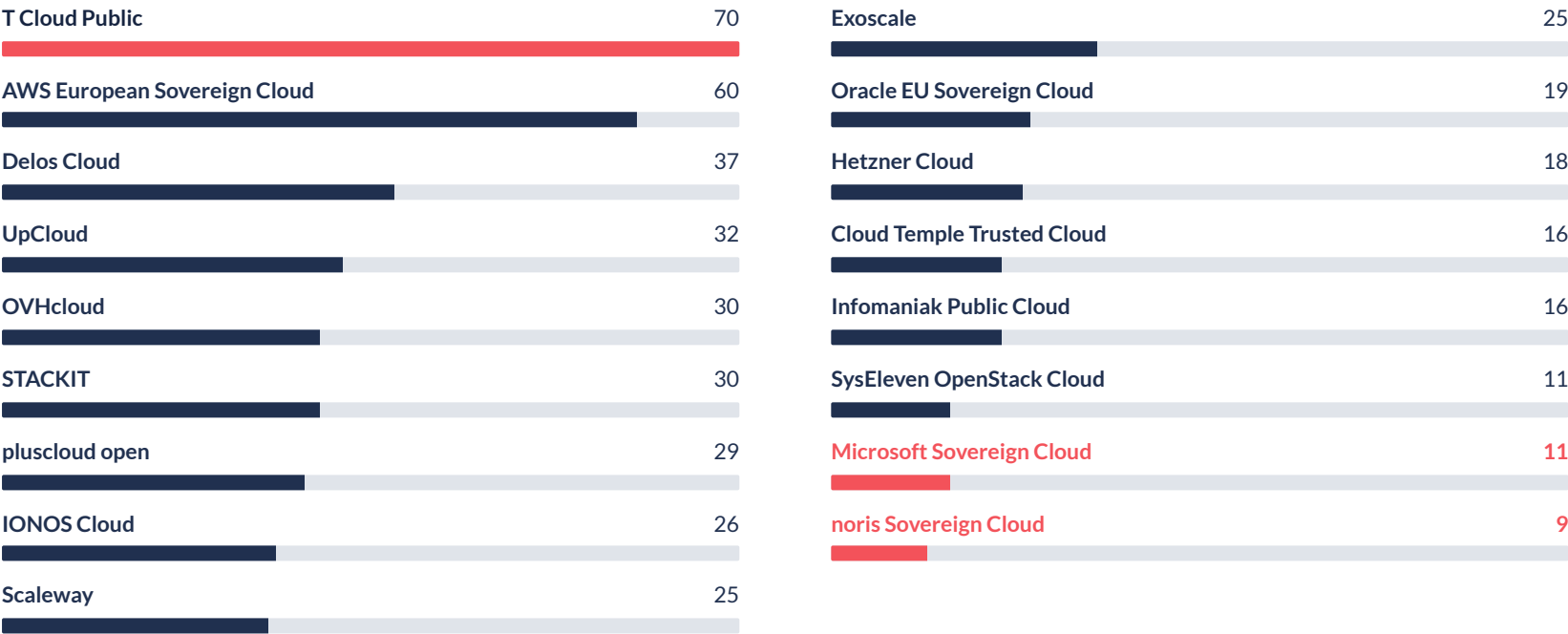
Bei 14 von 17 Anbietern fehlt ein dokumentiertes unabhängiges Beratungsgremium für Souveränitätsfragen. Nur AWS European Sovereign Cloud zeigt erste substanzielle Ansätze mit einem dokumentierten Governance-Board.

Die Transparenz-Lücke.

Transparenz & Prüfbarkeit erreicht mit 2,7/5 den zweitniedrigsten Marktdurchschnitt. Die Evidenzdichte variiert enorm: T Cloud Public ist mit 70 Quellen am besten dokumentiert; noris (9) und Microsoft (11) am schwächsten.

Evidenzdichte je Anbieter.

Anzahl öffentlich verlinkter Quellen-URLs. URL-Anzahl misst Breite, nicht Tiefe; jede Quelle ist im SCC einzeln auf belastbare Evidenz geprüft.



Drei kritische Kriterien.

Unabhängige Überprüfung (kontinuierlich) liegt bei 2,53/5, Blackbox-Risiko bei 2,59/5 und Richtliniendurchsetzung bei 2,53/5. Viele Anbieter betreiben Infrastruktur, deren Steuerungsebene (Control Plane) für den Kunden eine Blackbox bleibt. Transparenz korreliert nicht automatisch mit Qualität, aber ihre Abwesenheit ist ein messbares Risiko.

BEFUND 04 · VON 06

Dienstportfolio vs. Souveränität.

Die breitesten Portfolios gehören den Anbietern mit den niedrigsten Jurisdiktionswerten. Die Frage für Entscheider lautet: Ab welcher Portfoliotiefe wird Souveränität praktisch nutzbar?

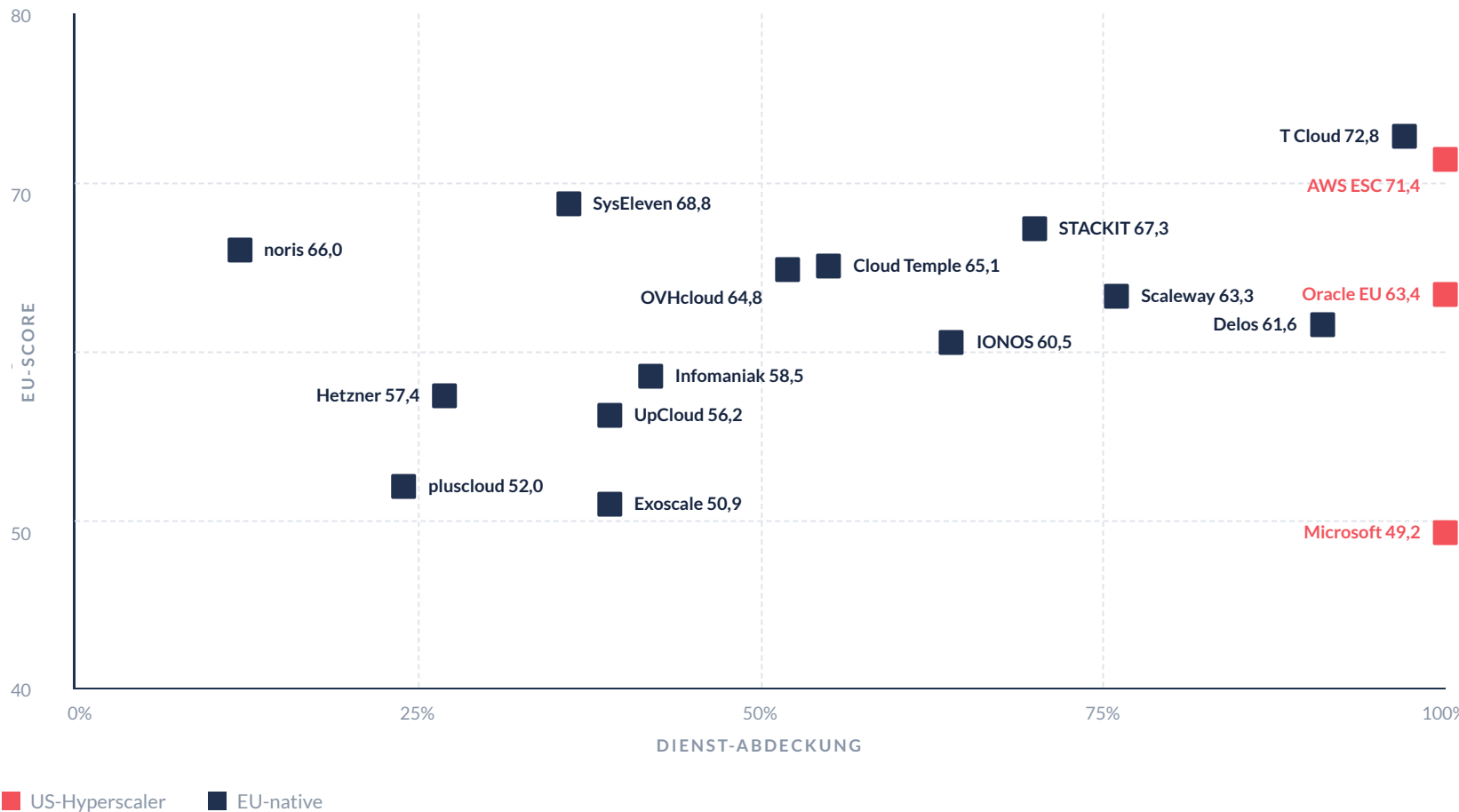
Für komplexe Enterprise-Workloads, die IAM, Container-Orchestrierung, Managed Databases und Observability erfordern, scheiden mehrere der nach Jurisdiktionskriterien führenden EU-Anbieter aus funktionalen Gründen aus. Das Dilemma ist real und wird sich erst lösen, wenn EU-native Anbieter ihre Portfolios ausbauen oder Kunden Multi-Cloud souverän umsetzen.

100% DIENST-ABDECKUNG	
ANBIETER	RECHT & JURISDIKTION
AWS European Sovereign Cloud	2,1
Oracle EU Sovereign Cloud	2,1
Microsoft Sovereign Cloud	0,9

12-27% DIENST-ABDECKUNG	
ANBIETER	RECHT & JURISDIKTION
noris Sovereign Cloud	4,3
pluscloud open	2,7
Hetzner Cloud	4,1

Portfolio-Souveränitäts-Matrix.

X-Achse: Dienst-Abdeckung (% der 33 bewerteten Dienste) · Y-Achse: EU-Souveränitätsscore (0–100). Rot = Hyperscaler, Navy = EU-native.



BEFUND 05 · VON 06

Compliance-Dynamik.

Zwischen SPOT-Revisionen 19 und 20 (Februar→März 2026) haben sich signifikante Score-Veränderungen ergeben.

ANBIETER	KRITERIUM	REV19	REV20	EREIGNIS
AWS European Sovereign Cloud	BSI C5	2	4	Typ 1 für 69 Services erreicht.
STACKIT	BSI C5	3	5	Typ 2 bestätigt.
T Cloud Public	Datenresidenz, BSI C5, Audit Evidence	↗	↗ ↗	Mehrere Score-Verbesserungen kumuliert.

Eine Momentaufnahme reicht nicht. Die Webapp wird laufend aktualisiert und reflektiert Score-Änderungen zeitnah.

BEFUND 06 · VON 06

Die ökonomische Dimension.

Souveränität hat einen Preis. Dieser Report quantifiziert ihn nicht direkt, aber die Daten erlauben eine strukturelle Einschätzung.

DIREKTE KOSTEN

+20–50%

Compute-Preise EU-nativer IaaS-Anbieter über vergleichbaren Hyperscaler-Instanzen. Geringere Skaleneffekte, höhere Compliance-Kosten, EU-basierte Betriebsstrukturen.

INDIREKTE KOSTEN

12–27%

Schmaleres Portfolio (noris 12%, Hetzner 27%) erfordert Multi-Cloud oder Eigenentwicklung für Dienste, die bei Hyperscalern Managed Service sind. Integrationskosten kompensieren oft die Einsparungen.

RISIKOKOSTEN

FISA 702?

Was kostet ein FISA-702-Disclosure? Ein fehlgeschlagenes BSI-Audit? Für KRITIS und Finanzsektor sind die Risikokosten mangelnder Souveränität potenziell höher als die Mehrkosten europäischer Anbieter.

Qualitative Einschätzung. Keine quantitative TCO-Analyse. Branchenspezifische Gewichtung erforderlich.

TEIL IV

Anbieterprofile.

17 Anbieter, alphabetisch sortiert. Jedes Profil zeigt das Souveränitätsprofil, EU-Score, SEAL-Näherung und Dienst-Abdeckung. Die vollständige Begründung jeder Einzelbewertung mit Quellenverweis liegt auf sovereigncloudcompass.de/anbieter/.

CLOUD SUITE

AWS European Sovereign Cloud.

Hyperscaler-Portfolio; EU sovereign partition / ops. GA seit 15. Jan. 2026, Region Brandenburg.

Technisch reifstes Profil im Feld (Portabilität 4,6, Audit Evidence 5/5, 100% Services), aber bei Recht & Jurisdiktion (2,1) durch US-Eigentümerschaft und FISA 702 strukturell gedeckelt.

71,4 EU- SCORE	SEAL 1 NÄHERUNG	100% ABDECKUNG	60 QUELLEN
Datenresidenz			
3,8			
Operationale Souveränität			
3,9			
Recht & Jurisdiktion			
2,1			
Kryptografie			
3,0			
Transparenz			
3,2			
Portabilität			
4,6			

CLOUD SUITE

Cloud Temple Trusted Cloud.

SecNumCloud-qualifizierte IaaS+PaaS Plattform (VMware/OpenIaaS + OpenShift PaaS); FR Souveränitätsfokus.

Einzigler durchgängig SecNumCloud-qualifizierter Anbieter (IaaS + PaaS). SEAL-0 durch niedrige Nachhaltigkeitswerte (SOV-8: 30%), nicht durch fehlende Souveränität.

65,1 EU- SCORE	SEAL 0 NÄHERUNG	55% ABDECKUNG	16 QUELLEN
Datenresidenz			
4,4			
Operationale Souveränität			
3,5			
Recht & Jurisdiktion			
4,1			
Kryptografie			
2,5			
Transparenz			
2,4			
Portabilität			
3,2			

FULL STACK

Delos Cloud.

Souveräne Azure/M365-Plattform für die deutsche Verwaltung (Betrieb in DE).

Einzigiger Full-Stack-Anbieter mit EU-Eigentümerschaft. D-Trust-Integration als Akzent. Transparenz (1,9) bleibt Schwachstelle.

61,6	SEAL 1	91%	37
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			3,9
Operationale Souveränität			3,4
Recht & Jurisdiktion			4,0
Kryptografie			2,5
Transparenz			1,9
Portabilität			2,9

IAAS+

Exoscale.

IaaS mit ausgewählten Managed Services (z.B. K8s/DB). Schweizer Holding.

Kompaktes IaaS+ aus der Schweiz mit Developer-Fokus und bestätigtem BSI C5 Typ 2 (4/5). Schweizer Jurisdiktion sowie fehlender IT-Grundschutz und fehlendes Confidential Computing begrenzen den DACH-Einsatz für regulierte Workloads.

50,9	SEAL 0	39%	25
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			3,0
Operationale Souveränität			2,1
Recht & Jurisdiktion			2,9
Kryptografie			1,5
Transparenz			2,7
Portabilität			3,2

IAAS

Hetzner Cloud.

Hetzner Cloud-Plattform (Console/API): Compute, Storage, Network, LB, K8s; ohne Dedicated/Colocation/Robot.

Preisgünstige EU-Infrastruktur mit starker Jurisdiktion (4,1) und vollständiger BSI-C5-Typ-2-Attestierung (5/5), aber ohne IT-Grundschutz, SecNumCloud und Confidential Computing.

57,4	SEAL 1	27%	18
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			3,0
Operationale Souveränität			2,2
Recht & Jurisdiktion			4,1
Kryptografie			1,5
Transparenz			2,9
Portabilität			2,7

IAAS+

Infomaniak Public Cloud.

OpenStack-basierte IaaS-Plattform (CH); Managed K8s/DBaaS/GPU/AI ergänzt; 100% CH-Betrieb.

100% Schweizer Betrieb mit eigenen Rechenzentren. Sehr niedrige Transparenz (1,6) und Kryptografie (1,5) im Feld.

58,5	SEAL 0	42%	16
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			3,1
Operationale Souveränität			2,7
Recht & Jurisdiktion			3,5
Kryptografie			1,5
Transparenz			1,6
Portabilität			3,1

IAAS

IONOS Cloud.

IaaS-Fokus (Compute/Storage/Network) mit selektiven Managed Services.

Moderates IaaS-Profil mit solider Portabilität (3,8) und bestätigtem BSI C5 Typ 1 (4/5). Begrenzte Kryptografie (1,5) und fehlendes Confidential Computing (1/5) sind Engpässe für regulierte Kunden.

60,5	SEAL 1	64%	26
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			2,9
Operationale Souveränität			2,3
Recht & Jurisdiktion			3,8
Kryptografie			1,5
Transparenz			2,9
Portabilität			3,8

FULL STACK

Microsoft Sovereign Cloud.

Azure + M365 Sovereignty Controls (Partner/Policies).

Ausgeprägtestes Ungleichgewicht im Feld: Portabilität 4,5 und Transparenz 3,6 bei Recht & Jurisdiktion 0,9. SOV-1 bei 0% determiniert den SEAL-0-Status.

49,2	SEAL 0	100%	11
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			3,2
Operationale Souveränität			2,7
Recht & Jurisdiktion			0,9
Kryptografie			2,0
Transparenz			3,6
Portabilität			4,5

IAAS+

noris Sovereign Cloud.

Souveräne Plattform/Services auf EU/DE-Betrieb; Scope je Produkt.

Attraktiv für KRITIS: starke Jurisdiktion (4,3) bei solider operationaler Souveränität. Geringe Evidenzdichte (9 URLs) und schmales Portfolio (12%).

66,0	SEAL 1	12%	9
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			3,9
Operationale Souveränität			3,2
Recht & Jurisdiktion			4,3
Kryptografie			2,5
Transparenz			2,9
Portabilität			3,4

CLOUD SUITE

Oracle EU Sovereign Cloud.

OCI Sovereign Cloud, breites IaaS+PaaS Portfolio.

Solide Datenresidenz (4,0) und operative Souveränität (3,9), aber niedrigste Transparenz im Feld (1,8) mit nur 19 Evidence-URLs. Aktiver Verbesserungsprozess läuft.

63,4	SEAL 1	100%	19
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			4,0
Operationale Souveränität			3,9
Recht & Jurisdiktion			2,1
Kryptografie			2,0
Transparenz			1,8
Portabilität			3,5

IAAS+

OVHcloud Public Cloud (inkl. SecNumCloud).

Public Cloud (IaaS/PaaS via OpenStack API) + SecNumCloud-qualifiziertes Bare Metal Pod; stark in IaaS/Infra.

SecNumCloud-Qualifizierung und EU-Eigentümerschaft als Differenzierung. Im DACH-Kontext fehlt BSI C5; Kryptografie (2,0) unter Marktdurchschnitt.

64,8 EU- SCORE	SEAL 1 NÄHERUNG	52% ABDECKUNG	30 QUELLEN
Datenresidenz			2,9
Operationale Souveränität			3,1
Recht & Jurisdiktion			3,8
Kryptografie			2,0
Transparenz			2,8
Portabilität			3,4

IAAS+

pluscloud open.

OpenStack/SCS-basierte IaaS-Plattform; Managed K8s/Platform-Services je Scope.

OpenStack-Basis mit solider Portabilität (3,3). Eigentümerstruktur drückt SOV-1 auf 10%. Schmales Portfolio (24%) begrenzt den Einsatzbereich.

52,0 EU- SCORE	SEAL 0 NÄHERUNG	24% ABDECKUNG	29 QUELLEN
Datenresidenz			3,2
Operationale Souveränität			3,0
Recht & Jurisdiktion			2,7
Kryptografie			2,0
Transparenz			2,9
Portabilität			3,3

CLOUD SUITE

Scaleway.

PaaS-breit (K8s/Serverless/DB etc.) plus IaaS.

Breites Cloud-Suite-Portfolio mit französischer EU-Eigentümerschaft. Operative Souveränität (2,3) und Kryptografie (1,5) fallen deutlich ab.

63,3	SEAL 1	76%	25
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			3,0
Operationale Souveränität			2,3
Recht & Jurisdiktion			4,1
Kryptografie			1,5
Transparenz			2,0
Portabilität			3,6

CLOUD SUITE

STACKIT.

Breites Portfolio (IaaS+PaaS), EU/DE-Fokus.

Starke operative Souveränität (3,9) mit bestätigtem C5 Typ 2 und Confidential Computing. Schwarz-Gruppe als Eigentümer ohne Non-EU-Abhängigkeiten.

67,3	SEAL 1	70%	30
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			3,2
Operationale Souveränität			3,9
Recht & Jurisdiktion			4,1
Kryptografie			2,0
Transparenz			3,4
Portabilität			3,2

IAAS+

SysEleven OpenStack Cloud.

OpenStack + ergänzende Managed Services / How-tos.

Höchste Transparenz unter EU-nativen Anbietern (3,9) mit starker Jurisdiktion (4,3). OpenStack liefert Portabilität, begrenzt aber das Portfolio (36%).

68,8	SEAL 1	36%	11
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			3,9
Operationale Souveränität			3,3
Recht & Jurisdiktion			4,3
Kryptografie			2,5
Transparenz			3,9
Portabilität			3,8

IAAS+

T Cloud Public.

Open Telekom Cloud / OpenStack-APIs; Managed Services ergänzt.

Ausgewogenstes Profil: einziger Anbieter ohne Achse unter 3,5. Höchster EU-Score (72,8) und einziger SEAL-2-Status. Referenzprofil für regulierte Organisationen.

72,8	SEAL 2	97%	70
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			4,2
Operationale Souveränität			3,6
Recht & Jurisdiktion			4,3
Kryptografie			3,5
Transparenz			3,6
Portabilität			3,6

IAAS

UpCloud.

IaaS-Fokus; Developer Tooling via API/IaC. Finnische EU-Jurisdiktion.

Solides IaaS aus Finnland mit EU-Jurisdiktion. Niedrigster Transparenz-Score im Feld (1,4); SEAL-0 durch fehlende Security-Compliance (SOV-7: 32,2%). Weder C5 noch SecNumCloud.

56,2	SEAL 0	39%	32
EU-SCORE	NÄHERUNG	ABDECKUNG	QUELLEN
Datenresidenz			3,0
Operationale Souveränität			3,1
Recht & Jurisdiktion			4,1
Kryptografie			1,5
Transparenz			1,4
Portabilität			3,3

Synopsis nach Anbieterklasse.

HYPERSCALER-TOCHTER

Stark in Technik, gedeckelt in Recht.

AWS ESC, Microsoft Sovereign Cloud, Oracle EU. Reife Portabilität (3,5–4,6), volle Dienstabdeckung (100%), aber Recht & Jurisdiktion deckelt bei 0,9–2,1.

EU-NATIVE · CLOUD SUITE / IAAS+

Ausgewogen, mit Ausreißern.

T Cloud, STACKIT, SysEleven, Cloud Temple. Recht & Jurisdiktion 4,1–4,3; Kryptografie/Confidential Computing bleibt für die meisten ein Hebel.

EU-NATIVE · REINE IAAS

Schmales Portfolio, hohe Jurisdiktion.

Hetzner, IONOS, UpCloud. EU-Eigentum 5/5 und FISA-702-Risiko 5/5; Compliance-Stack je nach Anbieter sehr unterschiedlich.

SCHWEIZ / SONDERFALL

CH-Jurisdiktion separat bewerten.

Exoscale, Infomaniak. CH-Souveränität rechtlich sauber, aber für DACH-Public-Sector und IT-Grundschutz nur partiell anwendbar.

TEIL V

Sektorspezifische Anwendungsfälle.

Der Compass liefert bewusst keinen generischen Gesamtsieger. Stattdessen bestimmt der Anwendungsfall die Gewichtung und die Mindestanforderungen. Vier Szenarien zeigen, wie unterschiedlich derselbe Datensatz ausfällt.

SZENARIO 1 · VON 4

Öffentliche Verwaltung / VS-NfD.

Fokus: Recht & Jurisdiktion (hohe Gewichtung), BSI C5 Typ 2 (≥4), IT-Grundschutz (≥3), EU-Eigentümerschaft (≥4). Die IT-Grundschutz-Anforderung wirkt als entscheidender zweiter Filter, mit einem Marktdurchschnitt von 1,24/5 ist sie ohnehin eines der schwächsten Kriterien.



ANBIETER	ERGEBNIS
IONOS Cloud	✓ ERFÜLLT
STACKIT	✓ ERFÜLLT
SysEleven OpenStack Cloud	✓ ERFÜLLT
AWS European Sovereign Cloud	Eigentümer 1/5, IT-Grundsch. 1/5, FISA 1/5
Cloud Temple Trusted Cloud	BSI C5 0/5, IT-Grundsch. 0/5
Delos Cloud	BSI C5 2/5, IT-Grundsch. 0/5
Exoscale	Eigentümer 3/5, IT-Grundsch. 1/5
Hetzner Cloud	IT-Grundsch. 0/5
Infomaniak Public Cloud	BSI C5 0/5, IT-Grundsch. 0/5
Microsoft Sovereign Cloud	Eigentümer 0/5, IT-Grundsch. 1/5, FISA 1/5
noris Sovereign Cloud	IT-Grundsch. 2/5
Oracle EU Sovereign Cloud	Eigentümer 1/5, BSI C5 2/5, IT-Grundsch. 0/5, FISA 1/5
OVHcloud Public Cloud	BSI C5 3/5, IT-Grundsch. 0/5
pluscloud open	Eigentümer 1/5, IT-Grundsch. 1/5
Scaleway	BSI C5 0/5, IT-Grundsch. 0/5
T Cloud Public	IT-Grundsch. 2/5
UpCloud	BSI C5 0/5, IT-Grundsch. 0/5

SZENARIO 2 · VON 4

KRITIS-Betreiber.

Fokus: Operationale Souveränität (hohe Gewichtung), keine kritischen Non-EU-Abhängigkeiten (≥3), EU-basierter Betrieb & Support (≥4), Datenresidenz (≥4). Die Anforderung an Non-EU-Abhängigkeiten filtert Anbieter mit unklarer Lieferkette. noris und T Cloud Public zeigen die stärksten Profile.

7

/17

ERFÜLLEN MINDESTANFORDERUNGEN

ANBIETER	ERGEBNIS
AWS European Sovereign Cloud	✓
Cloud Temple Trusted Cloud	✓
Delos Cloud	✓
Oracle EU Sovereign Cloud	✓
SysEleven OpenStack Cloud	✓
T Cloud Public	✓
noris Sovereign Cloud	✓

ANBIETER	AUSSCHLUSSGRUND
Exoscale	EU-Betrieb 2/5
Hetzner Cloud	EU-Betrieb 2/5
IONOS Cloud	EU-Betrieb 2/5
Microsoft Sovereign Cloud	Non-EU-Abh. 1/5
OVHcloud, STACKIT, Scaleway	Datenres. < 4
Infomaniak, UpCloud, pluscloud	Datenres. < 4

SZENARIO 3 · VON 4

Finanzsektor / BaFin-reguliert.

Fokus: Transparenz & Prüfbarkeit, Audit Evidence Pack (≥4), BSI C5 (≥3), Schlüsselhoheit (≥3), EU-Recht (≥4). AWS ESC schneidet trotz Jurisdiktionsschwäche überraschend stark ab, ein Beispiel dafür, dass Souveränitätsbewertung kontextabhängig ist.

8

/17

ERFÜLLEN MINDESTANFORDERUNGEN

ANBIETER	ERGEBNIS
AWS European Sovereign Cloud	✓
Exoscale	✓
Hetzner Cloud	✓
Microsoft Sovereign Cloud	✓
STACKIT	✓
SysEleven OpenStack Cloud	✓
T Cloud Public	✓
pluscloud open	✓

In der Marktrealität nutzen viele Finanzinstitute non-souveräne Hyperscaler mit kompensierenden Maßnahmen (BYOK/HYOK, Cloud-Exit-Pläne, regelmäßige DR-Tests); DORA und BaFin (BAIT/VAIT/MaRisk) fordern keine sovereign-cloud-native Architektur. Eine Verschärfung ergibt sich aus der BSI-Empfehlung zu Geo-Redundanz mit ≥200 km Abstand: Unter dieser Lesart fällt AWS ESC mit aktuell einer Region (Brandenburg) heraus, bis weitere EU-Regionen den GA-Status erreichen.

SZENARIO 4 · VON 4

Gesundheitswesen / gematik-Kontext.

Fokus: Datenresidenz (sehr hohe Gewichtung), Operator Access Exclusion (≥3), physisch/logische Trennung (≥3), EU-Eigentümerschaft (≥4), BSI C5 (≥4). Die gematik-Spezifikationen für ePA und TI 2.0 fordern keine hardwaregestützte TEE als Pflicht; das Szenario formuliert eine strikte Auslegung des Schutzbedarfs für besonders sensible Gesundheitsdaten.

1

/17

ANBIETER ERFÜLLT ALLE
MINDESTANFORDERUNGEN

Die Mindestanforderung Operator Access Exclusion ≥3 lässt mehrere Erfüllungswege zu: organisatorisch über sicherheitsüberprüftes Personal, vertraglich über Customer Lockbox oder technisch über Confidential Computing. Acht Anbieter erreichen den Schwellenwert; in Kombination mit EU-Eigentümerschaft (≥4), C5 (≥4) und durchgängiger Datenresidenz reduziert sich das Feld jedoch drastisch.

T Cloud Public – einziger Anbieter, der vollständig erfüllt.

STACKIT zeigt mit Confidential Server und Confidential Kubernetes (AMD SEV-SNP / Intel TDX, Score 4/5 bei Operator Access Exclusion) zwar das technologisch ausgereifteste Confidential-Computing-Profil im Feld, scheitert in diesem Szenario aber an physisch/logischer Trennung (2/5) und Datenresidenz (3,2/5).

Ausschlussgründe je Anbieter.

ANBIETER	AUSSCHLUSSGRUND
T Cloud Public	✓ ERFÜLLT
AWS European Sovereign Cloud	Eigentümer 1/5, Datenres. 3,8/5
Cloud Temple Trusted Cloud	Conf.Comp. 1/5, BSI C5 0/5
Delos Cloud	Conf.Comp. 2/5, BSI C5 2/5, Datenres. 3,9/5
Exoscale	Conf.Comp. 0/5, Phys.Trenn. 1/5, Eigentümer 3/5, Datenres. 3,0/5
Hetzner Cloud	Conf.Comp. 0/5, Phys.Trenn. 1/5, Datenres. 3,0/5
IONOS Cloud	Conf.Comp. 1/5, Phys.Trenn. 2/5, Datenres. 2,9/5
Infomaniak Public Cloud	Conf.Comp. 0/5, Phys.Trenn. 2/5, BSI C5 0/5
Microsoft Sovereign Cloud	Phys.Trenn. 2/5, Eigentümer 0/5, Datenres. 3,2/5
OVHcloud Public Cloud	Phys.Trenn. 2/5, BSI C5 3/5, Datenres. 2,9/5
Oracle EU Sovereign Cloud	Eigentümer 1/5, BSI C5 2/5
STACKIT	Phys.Trenn. 2/5, Datenres. 3,2/5
Scaleway	Conf.Comp. 0/5, Phys.Trenn. 1/5, BSI C5 0/5
SysEleven OpenStack Cloud	Conf.Comp. 1/5, Datenres. 3,9/5
UpCloud	Phys.Trenn. 1/5, BSI C5 0/5, Datenres. 3,0/5
noris Sovereign Cloud	Conf.Comp. 1/5, Datenres. 3,9/5
pluscloud open	Phys.Trenn. 2/5, Eigentümer 1/5

TEIL VI

EU-CSF-Referenzsicht.

Alle 31 Compass-Kriterien sind den acht Zielen des EU Cloud Sovereignty Framework (CSF v1.2.1) zugeordnet.

Die acht SOV-Ziele.

ZIEL	BEZEICHNUNG	GEW.	BESCHREIBUNG (EN)
SOV-1	Strategische Souveränität	15%	Strategic Sovereignty
SOV-2	Rechtliche & jurisdiktionelle Souveränität	10%	Legal & Jurisdictional Sovereignty
SOV-3	Daten- & KI-Souveränität	10%	Data & AI Sovereignty
SOV-4	Operationale Souveränität	15%	Operational Sovereignty
SOV-5	Lieferketten-Souveränität	20%	Supply Chain Sovereignty
SOV-6	Technologische Souveränität	15%	Technology Sovereignty
SOV-7	Sicherheits- & Compliance-Souveränität	10%	Security & Compliance Sovereignty
SOV-8	Ökologische Nachhaltigkeit	5%	Environmental Sustainability

SEAL-Näherung.

Die SEAL-Näherung ist eine konservative Proxy-Berechnung auf Basis der SCC-Daten und ausdrücklich keine offizielle EU-Zertifizierung. Berechnung folgt einem Minimum-Prinzip: Der SEAL-Wert eines Anbieters entspricht dem niedrigsten Wert über alle acht SOV-Ziele.

Schwellen: SEAL 4 ≥ 90%, SEAL 3 ≥ 75%, SEAL 2 ≥ 55%, SEAL 1 ≥ 40%, SEAL 0 < 40%. N/A wird als 0 gewertet, was den konservativen Charakter verstärkt.

SEAL-Verteilung.

SEAL	BEZEICHNUNG	ANZ.
SEAL 0	Keine Souveränität	6
SEAL 1	Jurisdiktionelle Souv.	10
SEAL 2	Datensouveränität	1
SEAL 3	Digitale Resilienz	0
SEAL 4	Vollständige Souv.	0

Warum haben sechs Anbieter SEAL 0?

SEAL 0 bedeutet nicht „keine Souveränität“. Es bedeutet, dass mindestens ein SOV-Ziel unter 40% liegt, das Minimum-Prinzip lässt eine einzelne Schwachstelle den Gesamtwert determinieren.

ANBIETER	ENGPASS-ZIEL	WERT	ERLÄUTERUNG
Cloud Temple Trusted Cloud	SOV-8	28%	Ökologische Nachhaltigkeit: PUE/CO2-Reporting unter Schwelle.
Infomaniak Public Cloud	SOV-7	32,8%	Sicherheits-Compliance: BSI C5/SecNumCloud unter Schwelle.
UpCloud	SOV-7	32,2%	Sicherheits-Compliance: BSI C5/SecNumCloud unter Schwelle.
pluscloud open	SOV-1	13,3%	Strategische Souveränität: Eigentümer/Advisory Board unter Schwelle.
Exoscale	SOV-1	40%	Strategische Souveränität: Eigentümer/Advisory Board unter Schwelle.
Microsoft Sovereign Cloud	SOV-1	0%	Strategische Souveränität: Eigentümer 0/5, kein Advisory Board.

TEIL VII

Ausblick und offene Fragen.

EUCS und die Zukunft der EU-Cloud-Regulierung.

Das European Cybersecurity Certification Scheme for Cloud Services (EUCS) befindet sich weiterhin in der Abstimmung. Die zentrale Streitfrage bleibt: Wird das Schema Souveränitätsanforderungen auf den höchsten Zertifizierungsstufen vorsehen, die US-Hyperscaler strukturell ausschließen? Oder wird ein technischer Ansatz gewählt, der Operational Measures als hinreichend akzeptiert? Die Entscheidung wird die Marktdynamik fundamental prägen.

Confidential Computing als Game Changer.

Hardwaregestützte Workload-Isolation hat das Potenzial, die Souveränitätsdebatte zu verändern. AWS setzt mit Nitro System und Nitro Enclaves einen Ansatz um, der den Betreiberzugriff technisch einschränkt (4/5). AMD SEV-SNP und Intel TDX ermöglichen darüber hinaus VM-Level Isolation, die STACKIT mit Confidential Server implementiert hat. Wenn der Betreiber technisch nachweisbar keinen Zugriff hat, verschiebt sich die Jurisdiktionsfrage: Nicht mehr, ob ein Zugriff verlangt werden kann, sondern ob er technisch lieferbar wäre.

AI-Souveränität: Die nächste Dimension.

Wo werden Modelle trainiert und inferenziert? Wer kontrolliert die Trainingsdaten? Unterliegen die Inferenzergebnisse denselben Residenz- und Jurisdiktionsanforderungen wie die Eingabedaten? Eine vertiefte Souveränitätsbewertung für KI-spezifische Kriterien steht als Erweiterung an.

Marktkonsolidierung und neue Anbieter.

Neue Anbieter wie Uptime IT (Hamburg, BSI C5 Typ 2, eigene Rechenzentren) stehen zur Bewertung an. Gleichzeitig ist Konsolidierung absehbar: Nicht alle 17 Anbieter werden dauerhaft als eigenständige souveräne Angebote bestehen.

Von der Analyse zur Entscheidung.

Dieser Report liefert eine Momentaufnahme. Die Webapp unter sovereigncloudcompass.de ermöglicht die individuelle Konfiguration von Gewichtungen und Mindestanforderungen. Der Compass ist ein Analysewerkzeug, kein Zertifizierungsprogramm.

“Souveränität ist kein Standardprodukt, sondern eine strategische Entscheidung mit individuellen Konsequenzen. Der Compass macht die Konsequenzen messbar.”

ANHANG A

Kriterienkatalog.

Alle 31 Bewertungskriterien mit Standardgewichtung, Marktdurchschnitt und Erläuterung. Gewichtung individuell anpassbar auf sovereigncloudcompass.de.

KRITERIUM	GEW.	Ø MARKT	WARUM WICHTIG?
Dienstportfolio-Tiefe	3	3,58	Viele Sovereignty-Programme scheitern an fehlenden Managed Services.
Integrierter Sicherheits-Stack	2	3,07	Identity → KMS → Logging/Monitoring → Network Security.
Energieeffizienz / PUE	2	3,65	Energieeffiziente Infrastruktur und messbare Verbesserungsziele.
CO ₂ /Wasser-Reporting	3	3,65	Transparente Offenlegung + low-carbon Sourcing.
Kundeninhalte in der EU	5	4,18	Regulatorische Anforderungen an Datenresidenz.
Kundenerstellte Metadaten in der EU	4	3,44	Metadaten können sensitiv sein (Tags, Ressourcennamen).
Physisch & logisch getrennt	4	2,41	Reduziert Risiko durch Plattform-/Admin-Abhängigkeiten.
Geografische Abdeckung & Redundanz	3	3,71	Failure Domains, Geo-Redundanz, DR innerhalb EU/DE.
EU-basierter Betrieb & Support	5	3,88	Souveränität erfordert operative Kontrolle.
Keine kritischen Non-EU Abhängigkeiten	4	3,47	Krisenszenarien / geopolitische Risiken.
Richtliniendurchsetzung (Leitplanken)	3	2,53	Technische Durchsetzung verhindert Fehlkonfiguration.
Standardmäßig verweigert / Sicher ab Werk	2	2,76	Sichere Defaults reduzieren Risiko und Audit-Aufwand.
Ausschluss von Betreiberzugriff	3	1,94	TEEs/Attestation/Schlüsselhoheit für hochregulierte Daten.
Eigentümerstruktur (EU-Inhaberschaft)	4	3,82	Beeinflusst Zugriffspflichten (CLOUD Act) und Governance.
Beherrschender Einfluss & FISA-702	5	4,12	Juristischer Durchgriff trotz technischer Datenresidenz.
Lokale Vertragseinheit & EU-Governance	4	3,82	Klare Verantwortlichkeiten für Betrieb/Support.
Unabhängiges Beratungsgremium	2	0,47	Zusätzliche Kontrolle für Souveränitätsentscheidungen.
EU-Stammzertifizierungsstelle	3	1,59	PKI/Trust für Identität, TLS, Signaturen.
Blackbox-Risiko (Control Plane)	3	2,59	Operative Blackbox begrenzt klassische Auditfähigkeit.
BSI C5	4	3,00	Wichtig für DE Public Sector und regulierte Industrien.
ISO 27001 / ISMS	3	3,82	Basis-Zertifikat; oft Ausschreibungs-Muss.
IT-Grundschutz (BSI)	3	1,24	Für deutsche Behörden / High-Trust Workloads.
SecNumCloud (ANSSI)	2	0,76	Französisches High-Trust Label (OIV/OSE).
Prüfberichte / Nachweispaket	4	3,71	Ohne Evidence scheitert die Prüfung.
Unabhängige Überprüfung (kontinuierlich)	2	2,53	Wirkung statt Papier; reduziert Blind Spots.
Offene Standards / API-Portabilität	3	3,59	Reduziert Lock-in, erleichtert Multi-Provider.
IaC & Automatisierung	5	4,12	Reproduzierbarkeit, Compliance-as-Code.
SDLC/DevOps im Alltag	4	3,29	Build, Deploy, Rollback, Secrets, Container.
Beobachtbarkeit (Logs/Metriken/Traces)	4	3,35	Kernbaustein für regulierte Workloads.
Limits/Quotas (Transparenz & Erhöhung)	2	2,76	Hidden Limits sind häufige Go-Live-Blocker.
Referenzarchitekturen / Landing Zones	2	2,65	Beschleunigen sichere Standardisierung.

ANHANG B

Rechtliche Hinweise und Nutzungsbedingungen.

0. Adressatenkreis (B2B).

Dieser Report richtet sich ausschließlich an Unternehmer im Sinne von § 14 BGB. Verbraucher im Sinne von § 13 BGB sind von der Nutzung ausgeschlossen.

1. Charakter des Reports.

Dieser Report ist ein Informations- und Vergleichsdokument. Er stellt keine Empfehlung, kein Angebot und keine Beratung dar. Die enthaltenen Bewertungen sind eine modellbasierte Auswertung auf Basis hinterlegter Daten und Gewichtungen. „Souveränität“ ist kontextabhängig und hängt u.a. von Vertrag, Geltungsbereich, Betriebsmodell, Auditnachweisen, Unterauftragsverarbeitern und Governance ab.

2. Verantwortung und Geltungsbereich.

Der Compass ersetzt keine rechtliche oder organisatorische Vorprüfung. Die Verantwortung für Zulässigkeit, Risikoakzeptanz und Haftung liegt ex ante beim Cloud-Nutzer.

3. Datenbasis, Quellen und Aktualität.

Die Informationen stammen aus öffentlich zugänglichen Quellen und/oder Herstellerangaben, die im Compass als Nachweise verlinkt werden. Cloud-Angebote ändern sich laufend. Inhalte können daher unvollständig, missverständlich oder veraltet sein.

4. Keine Gewähr.

Soweit gesetzlich zulässig, erfolgen alle Inhalte ohne Gewähr für Richtigkeit, Vollständigkeit und Aktualität. Bewertungen, Abdeckungsgrade, SEAL-Näherungswerte und Zertifikatsangaben ersetzen keine Prüfung von Vertrag, Geltungsbereich, Auditnachweisen und Betriebsmodell im konkreten Anwendungsfall.

5. Haftung.

Wir haften unbeschränkt bei Vorsatz und grober Fahrlässigkeit sowie bei Schäden aus der Verletzung von Leben, Körper oder Gesundheit. Bei einfacher Fahrlässigkeit haften wir nur bei Verletzung wesentlicher Vertragspflichten (Kardinalpflichten) und beschränkt auf den typischerweise vorhersehbaren Schaden. Im Übrigen ist die Haftung, soweit gesetzlich zulässig, ausgeschlossen.

6. Externe Links.

Quellenlinks verweisen auf externe Websites. Für deren Inhalte und Datenverarbeitung sind die jeweiligen Betreiber verantwortlich.

7. Marken und Neutralität.

Alle genannten Anbieter- und Produktnamen können Marken der jeweiligen Rechteinhaber sein. Dieser Report enthält keine bezahlten Platzierungen und keine Empfehlungen.

IMPRESSUM

HERAUSGEBER

Jörn Petereit

IT Capital Partners GmbH
Ballindamm 3, 20095 Hamburg
HRB 183093

KONTAKT

joern@itcapital.de

Datenquelle: Sovereign Cloud Compass
SPOT Revision 20, Stand März 2026.

FINANZIERUNG

Eigenfinanziert.

Keine Zahlungen, Sponsorings, Werbe- oder Provisionsbeziehungen mit bewerteten Anbietern.