SOUVERÄN GEMACHT

Souveränität einkaufen: Woran Sie sie in der Ausschreibung erkennen

Von **Thomas Faß** · 28. Oktober 2026



Ausgabe 7 · 28. Oktober 2026 · Thomas Faß. Diese Ausgabe ordnet Vergaberecht und Kriterienkataloge ein und ersetzt keine Rechtsberatung.

In Kürze

- Die Schweiz hat am 20. Oktober 2026 ihre Government Cloud ausgeschrieben: drei Lose, gestaffelt nach Schutzbedarf, und kein Anbieter darf mehr als ein Los gewinnen [1].
- Die EU-Kommission hat für ihre eigene Cloud-Beschaffung Souveränität in acht Ziele zerlegt und je Ziel eine Mindeststufe verlangt. Drei von vier Zuschlägen erreichten die zweithöchste Stufe [4][6].
- In Deutschland nennt die Vergabeverordnung seit dem 1. Juli 2026 „Aspekte der digitalen Souveränität“ als mögliches Zuschlagskriterium [13][15]. Was darunter fällt, lässt das Gesetz offen.
- Für die Lücke gibt es Werkzeuge: den BSI-Katalog C3A, den EU-Rahmen mit seinen Stufen und für den Ausstieg die Vertragsmuster EVB-IT Cloud [10][4][16].
- Eine von Microsoft unterstützte Studie zeigt das Risiko: Wo neuere Souveränitätsrahmen in Ausschreibungen stehen, gab es öfter nur einen Bieter [8].

Die Schweiz kauft Cloud in drei Stufen

Das Bundesamt für Informatik hat die Swiss Government Cloud in drei Losen ausgeschrieben, die drei Cloud-Stufen entsprechen [1]. Die Ausschreibung gehört zum Programm Swiss Government Cloud, das der Bund von 2025 bis 2032 aufbaut [3]. Los 1 ist eine globale Public Cloud. Los 2 ist eine Public Cloud mit

Datenhaltung und Datenbearbeitung ausschließlich in der Schweiz, auf Basis von Open-Source-Lösungen. Los 3 ist eine Private Cloud in den Rechenzentren des Bundes, für besonders schutzwürdige Anwendungen.

Zwei Regeln verdienen Aufmerksamkeit. Erstens die Losbeschränkung: Ein Anbieter kann nur für ein Los einen Zuschlag erhalten. Los 1 und Los 2 gehen an je zwei Anbieter, Los 3 an einen, zusammen also fünf Zuschläge [1]. Der Bund begründet das damit, die Abhängigkeit von einzelnen Anbietern und Jurisdiktionen zu verringern [1]. Zweitens das Volumen: Bis zu 7 Milliarden Franken über 14 Jahre sind als optionale Obergrenze formuliert. Abgerechnet wird nur, was genutzt wird, und alle sieben Jahre öffnet sich der Markt neu [1].

Welche Daten in welche Stufe dürfen, regeln die Cloud-Prinzipien der Bundesverwaltung, in Kraft seit 1. Januar 2026 [2]. Als „geheim“ klassifizierte Daten dürfen weder in die beiden Public-Cloud-Stufen noch in die Private Cloud der Stufe III. Für Public-Cloud-Vorhaben muss die zuständige Stelle je Vorhaben eine Exit-Strategie festlegen [2]. Die Reihenfolge ist damit klar: erst der Schutzbedarf, dann die Stufe, dann der Anbieter.

Die EU-Kommission hat Souveränität benotet

Für eine eigene Ausschreibung über bis zu 180 Millionen Euro hat die EU-Kommission im Oktober 2025 ein „Cloud Sovereignty Framework“ veröffentlicht [4][5]. Es zerlegt Souveränität in acht Ziele, jeweils mit Gewicht: Strategie 15 %, Recht und Gerichtsbarkeit 10 %, Daten und KI 10 %, Betrieb 15 %, Lieferkette 20 %, Technologie 15 %, Sicherheit und Compliance 10 %, Nachhaltigkeit 5 % [4].

Jedes Ziel wird auf einer Skala von SEAL-0 („No Sovereignty“) bis SEAL-4 („Full Digital Sovereignty“) eingestuft. Die Ausschreibung legt je Ziel eine Mindeststufe fest. Wer sie verfehlt, scheidet aus. Die gewichtete Summe geht danach als Zuschlagskriterium in die Wertung ein [4].

Im April 2026 hat die Kommission vier Verträge vergeben. Mindestens verlangt war SEAL-2, drei Anbieter erreichten SEAL-3, einer SEAL-2 [6]. Die Kommission empfiehlt den Rahmen inzwischen ausdrücklich auch Behörden und Unternehmen [7].

Daneben läuft ein Gesetzgebungsverfahren: Der Vorschlag für einen Cloud and AI Development Act vom 3. Juni 2026 sieht einen eigenen EU-Rahmen mit vier Prüfstufen vor, von der Selbstbewertung des Anbieters bis zur Prüfung durch Dritte [17]. Die Stufen dieses Vorschlags und die SEAL-Skala der Kommission sind zwei verschiedene Systeme. Wer sie in einer Ausschreibung verwendet, sollte das auseinanderhalten.

Was eine Studie über Souveränitätsklauseln zeigt

Das Brüsseler Institut ECIPE hat 8.725 vergebene Cloud-Lose aus neun Mitgliedstaaten von 2018 bis 2025 ausgewertet [8]. Ohne Souveränitätssprache gingen rund 92 % der Aufträge an inländische Anbieter. Bei Ausschreibungen, die neuere Rahmen wie C5 oder vergleichbare nationale Kataloge nennen, waren es 100 % [8]. Der Anteil der Verfahren mit nur einem Bieter stieg dort von 28 % auf 46 % [8].

Zwei Einschränkungen gehören dazu. Die Werte zu den neueren Rahmen beruhen auf einer kleinen Basis, nach Angabe der Autoren 22 Bekanntmachungen mit Bieterdaten [8]. Und die Studie entstand mit Unterstützung von Microsoft [8]. Sie zeigt einen Zusammenhang. Dass die Klauseln den Wettbewerb verdrängt haben, belegt sie nicht.

Die Autoren selbst ziehen eine brauchbare Linie: Souveränität solle sich am nachgewiesenen Ergebnis messen lassen. Die Eigentümerstruktur des Anbieters allein reiche dafür nicht [8]. Echte Souveränität heißt nach ECIPE-Direktor Fredrik Erixon, dass ein öffentlicher Auftraggeber zeigen kann, dass seine Daten sicher sind und dass er den Anbieter wechseln kann, wenn er muss [9]. Das ist ein Prüfauftrag. Ein Etikett erfüllt ihn nicht.

Deutschland: Souveränität ist Zuschlagskriterium, aber ohne Inhalt

Mit dem Gesetz zur Beschleunigung der Vergabe öffentlicher Aufträge, in Kraft seit dem 1. Juli 2026, haben zwei Normen die digitale Souveränität aufgenommen [15]. § 58 Abs. 2 der Vergabeverordnung nennt „Aspekte der digitalen Souveränität“ als mögliches Zuschlagskriterium [13]. § 128 Abs. 2 GWB erlaubt Ausführungsbedingungen, die „Belange der Versorgungssicherheit oder der digitalen Souveränität“ betreffen [14].

Was diese Aspekte sind, sagt der Gesetzestext nicht. Interoperabilität, offene Standards oder Open Source stehen dort nicht [13][14]. Die Vergabestelle muss die Kriterien selbst bestimmen, und sie müssen mit dem Auftrag zusammenhängen. Genau hier helfen die Kataloge.

Für Unternehmen gilt das Vergaberecht nicht. Die Logik lässt sich trotzdem übernehmen, und die Werkzeuge stehen jedem offen.

Grundlagen: Souveränität prüfbar machen in vier Stufen

1. Schutzbedarf vor Anbieter. Wie in der Schweiz steht am Anfang die Frage, welche Daten in die Cloud sollen und wie schutzbedürftig sie sind. Öffentliche Dokumentation braucht andere Kriterien als Kundendaten oder Betriebsdaten kritischer Infrastruktur. Erst danach lässt sich sagen, welche Stufe nötig ist.

2. Mindestniveau je Dimension. Der BSI-Katalog C3A („Criteria enabling Cloud Computing Autonomy“) vom 27. April 2026 übernimmt Aufbau und Ziele des EU-Rahmens [10][11]. Er klammert Sicherheit und Compliance aus, weil C5 und IT-Grundschutz sie abdecken, und Nachhaltigkeit, weil sie nicht in die Zuständigkeit des BSI fällt [11]. Der Katalog besteht aus Kriterien und Zusatzkriterien, aus denen Kunden je nach Anwendungsfall wählen [11]. Ein Beispiel aus der Mitteilung des BSI: Je nach Risikoanalyse kann der Kunde für den Standort der Rechenzentren und die Herkunft des Betriebspersonals eine Lokalisierung in Deutschland oder in der EU verlangen [10].

3. Nachweis vor Zusage. C3A setzt voraus, dass der Anbieter die C5-Kriterien erfüllt [10]. C5 ist ein Kriterienkatalog. Ein Zertifizierungsverfahren gibt es dafür nicht, den Nachweis liefert ein Testat eines Wirtschaftsprüfers [12]. Die neue Fassung C5:2026 gilt für Testate mit Stichtag oder Berichtszeitraum ab dem 1. Juni 2027, eine frühere Anwendung ist erlaubt [12]. Auch C3A ist für sich nicht verbindlich. Anbieter können die Einhaltung per Audit nachweisen, ein Leitfaden dafür ist angekündigt [10][11]. Eine Selbstauskunft ist die schwächste Form des Nachweises.

4. Ausstieg im Vertrag. Den Wechsel deckt C3A ausdrücklich nicht ab. Das BSI verweist dafür auf den Abschnitt Portabilität und Interoperabilität in C5:2026 [11]. Konkrete Vertragsregeln liefern die EVB-IT Cloud-AGB: Daten werden ohne gesonderte Vergütung herausgegeben, der Weiterbetrieb über das Vertragsende hinaus ist bis zu sechs Monate möglich, der Export bleibt bis zu drei Monate nach Vertragsende möglich, und das Format muss marktüblich sein [16]. Wie der Data Act den Wechsel zusätzlich regelt, beschreibt Ausgabe 6.

Vier Größen für Ihre nächste Ausschreibung

1. **Schutzbedarf je Datenklasse.** Eine Zeile pro Datenklasse, mit der Stufe, die sie braucht. Alles Weitere leitet sich daraus ab.
2. **Ausschluss oder Punkte.** Welche Kriterien sind Mindestanforderung, welche fließen gewichtet in die Wertung ein? Die EU-Kommission hat beides kombiniert [4].
3. **Nachweisform.** Testat, Audit oder Selbstauskunft, je Kriterium festgelegt, bevor die Angebote kommen.
4. **Exit-Fristen.** Exportfrist, Datenformat und Weiterbetrieb nach Vertragsende, als Zahl im Vertrag.

Drei Fragen für das nächste Anbietergespräch

1. Welchem Recht unterliegt der Betreiber, und von wo aus administriert Personal die Systeme, auf denen unsere Daten liegen?
2. Liegt ein aktuelles C5-Testat vor, und wer hat die Souveränitätszusagen geprüft: Sie selbst, oder ein unabhängiger Prüfer nach C3A oder dem EU-Rahmen?
3. Wie lange können wir nach Vertragsende exportieren, in welchem Format, und was kostet die Unterstützung dabei?

Zusatz für die Praxis

Strengere Kriterien verkleinern den Kreis der Bieter. Das zeigt die ECIPE-Auswertung, und es ist im Mittelstand nicht anders [8]. Die Schweiz löst das über Stufen: Nicht jede Anwendung muss in die strengste. Für ein Unternehmen heißt das, die strengsten Kriterien nur dort zu verlangen, wo die Datenklasse es rechtfertigt. Die Losbeschränkung lässt sich im Kleinen ebenfalls übertragen: zwei Anbieter für zwei Datenklassen. Das kostet Integrationsaufwand und senkt die Abhängigkeit. Abwägen müssen Sie beides selbst.

Zahlen

- **3 Lose, 5 Zuschläge, 1 Los je Anbieter:** Swiss Government Cloud, Ausschreibung vom 20.10.2026 [1].
- **Bis zu 7 Mrd. CHF über 14 Jahre:** optionale Obergrenze, Los 1 und 2 je bis zu 2 Mrd., Los 3 bis zu 3 Mrd. [1].
- **8 Ziele, Skala SEAL-0 bis SEAL-4:** EU Cloud Sovereignty Framework, größtes Gewicht Lieferkette mit 20 % [4].
- **Bis zu 180 Mio. Euro, 4 Verträge, 3 × SEAL-3:** Cloud-Ausschreibung der EU-Kommission, Zuschlag April 2026 [5][6].
- **8.725 Cloud-Lose, 9 Mitgliedstaaten, 2018–2025:** ECIPE-Auswertung [8].
- **28 % → 46 %:** Anteil der Verfahren mit nur einem Bieter, ohne Souveränitätssprache gegenüber neueren Rahmen (kleine Basis, 22 Bekanntmachungen mit Bieterdaten) [8].
- **1. Juni 2027:** ab diesem Stichtag gilt C5:2026 für Testate [12].
- **6 und 3 Monate:** Weiterbetrieb und Exportfrist nach Vertragsende in den EVB-IT Cloud-AGB [16].

Der Gedanke zum Mitnehmen

Souveränität steht inzwischen in Ausschreibungen, im Gesetz und in Katalogen. Prüfbar wird sie erst, wenn drei Dinge festliegen: welche Daten welchen Schutz brauchen, welches Niveau je Dimension reicht und wie der Anbieter es nachweist. Sovereign by design heißt für uns, diese drei Fragen vor der Architektur zu beantworten. Was ohne Nachweis zugesagt wird, bleibt ein Etikett.

Diesen Newsletter schreibt Thomas Faß, Gründer von InnoShore aus Münster. InnoShore stellt Senior-IT-Experten bereit und liefert schlüsselfertige IT-Lösungen für den DACH-Mittelstand — mit Senior-Steuerung in Deutschland und einem Compliance-Baukasten, der pro Mandat konfiguriert wird, nicht von der Stange kommt.

Quellen

[1] *Swiss Government Cloud: Ausschreibung gestartet*. Der Bundesrat / Bundesamt für Informatik, Medienmitteilung, 20.10.2026.

[2] *AR010 Cloud-Prinzipien der Bundesverwaltung, V1.2*. Schweizerische Bundeskanzlei, Bereich Digitale Transformation und IKT-Lenkung, beschlossen 10.12.2025, in Kraft 01.01.2026.

[3] *Swiss Government Cloud (SGC)*. Bundesamt für Informatik, Programmseite.

[4] *Cloud Sovereignty Framework, Version 1.2.1*. Europäische Kommission, GD Informatik, Oktober 2025.

[5] *Commission moves forward on cloud sovereignty with EUR 180 million tender*. Europäische Kommission, Meldung, 10.10.2025.

[6] *Commission advances cloud sovereignty through strategic procurement*. Europäische Kommission, Meldung, 17.04.2026.

[7] *Sovereign Cloud Framework explained*. Europäische Kommission, Meldung, 01.06.2026.

[8] *Cloud Sovereignty and the Single Market*. Matthias Bauer, Andrea Dugo, Fredrik Erixon, Dyuti Pandya, Elena Sisto, ECIPE Occasional Paper 09/2026, Oktober 2026, erstellt mit Unterstützung von Microsoft.

[9] *ECIPE-Pressemitteilung zum Occasional Paper 09/2026*. ECIPE, 19.10.2026.

[10] *C3A: BSI veröffentlicht Souveränitätskriterien für Cloud-Dienste*. Bundesamt für Sicherheit in der Informationstechnik, Pressemitteilung, 27.04.2026.

[11] *C3A – Criteria enabling Cloud Computing Autonomy*. Bundesamt für Sicherheit in der Informationstechnik, Themenseite.

[12] *Kriterienkatalog C5: Häufige Fragen*. Bundesamt für Sicherheit in der Informationstechnik.

[13] *§ 58 Vergabeverordnung (VgV): Zuschlag und Zuschlagskriterien*. Bundesministerium der Justiz, gesetze-im-internet.de.

[14] *§ 128 Gesetz gegen Wettbewerbsbeschränkungen (GWB): Auftragsausführung*. Bundesministerium der Justiz, gesetze-im-internet.de.

[15] *Gesetz zur Beschleunigung der Vergabe öffentlicher Aufträge*. Bundesgesetzblatt 2026 I Nr. 137, 18.05.2026.

[16] *EVB-IT Cloud – Allgemeine Geschäftsbedingungen, Version 1.0*. IT-Planungsrat, Beschluss 2022/01.

[17] *Proposal for a Regulation on the Cloud and AI Development Act, COM(2026) 502 final*. Europäische Kommission, 03.06.2026, Ratsdokument 10104/26.

Alle Ausgaben von „Souverän gemacht" finden Sie unter innoshore.de/souveraenitaet. Die vorige Ausgabe: Cloud-Exit: Ab dem 12. Januar 2027 kostet der Wechsel kein Entgelt mehr.

Verwandte Inhalte

- Souveräne KI-Entwicklung: Datenklassen, Inferenz und Regulierung
- Ausgabe 6: Cloud-Exit ohne Wechselentgelte
- Cloud-Governance & Compliance

SOUVERÄN GEMACHT

Den Newsletter abonnieren

Lesen Sie jede Ausgabe zu KI-Governance und digitaler Souveränität direkt in Ihrem Feed — über unseren LinkedIn-Newsletter „Souverän gemacht".

Newsletter auf LinkedIn abonnieren

Die Anmeldung zum Newsletter direkt hier auf der Seite steht in Kürze zur Verfügung.