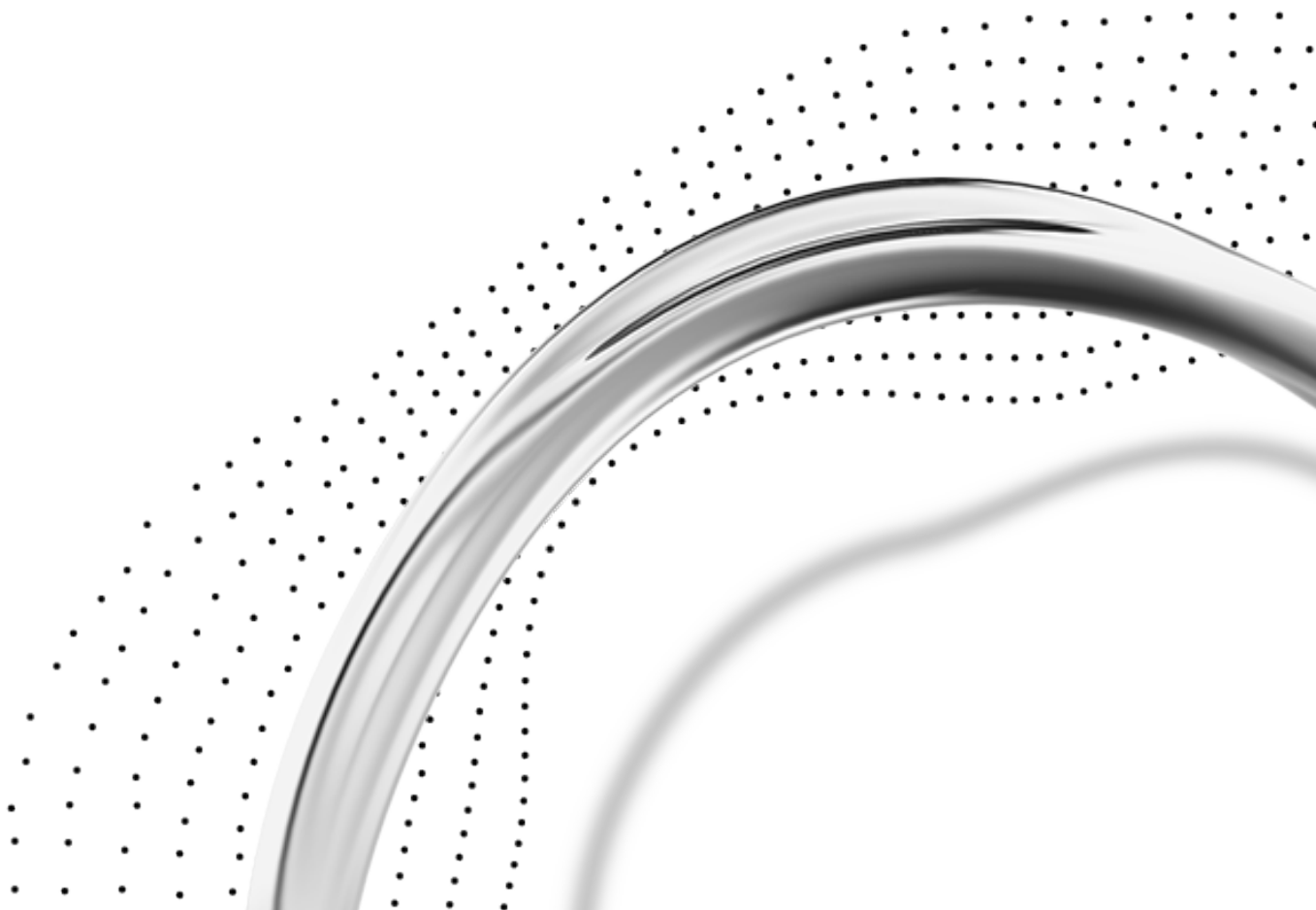


Version 1.0

Kriterien zur Bewertung von Digitaler Souveränität

– aus messbar wird machbar



Inhalt

Executive Summary	3
„Aus messbar wird machbar“: eine Konsultation mit messbarem Ergebnis	4
1. Gestaltungsfähigkeit	5
2. Operationalisierung und Nachweise	6
3. Gewichtung - ja oder nein?	7
4. Rolle von Open Source	8
5. Konsolidierung mit bestehenden Frameworks (EU CSF und C3A)	9
Kriterien und Anwendung	10
Kriterienkatalog - Organisation	11
Kriterienkatalog - IT	12

Executive Summary

Um die Digitale Souveränität der Öffentlichen Verwaltung gezielt zu steuern und zu stärken, muss Souveränität anhand klarer Kriterien messbar sein. Bislang fehlten der öffentlichen Hand solche Kriterien. Daher hat das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) einen Kriterienkatalog zur Bewertung Digitaler Souveränität von Behörden vorgeschlagen und im Rahmen einer öffentlichen Konsultation weiterentwickelt. Das Ergebnis ist ein praxisnahes Framework, das sowohl die strategische und organisatorische Souveränität einer Verwaltung als auch die ihrer geschäftskritischen IT-Lösungen bewertet. Klare Prüffragen und Nachweise schaffen Transparenz und Vergleichbarkeit. Kritische Defizite werden zudem durch eine Gate-Logik in der Bewertung sichtbar.

Die überarbeiteten Kriterien stärken insbesondere die Gestaltungsfähigkeit der Verwaltung und schließen an bestehende Rahmenwerke wie das EU Cloud Sovereignty Framework an. Sie bieten Behörden einen einfach anwendbaren Einstieg, um Abhängigkeiten zu identifizieren und strategische Entscheidungen für eine souveräne digitale Infrastruktur zu treffen.

„Aus messbar wird machbar“: eine Konsultation mit messbarem Ergebnis

Je stärker ihre Digitale Souveränität gefährdet ist, desto mehr müssen Verwaltungen in sie investieren. Darauf reagiert der Markt: Es gibt vermehrt Angebote, die Souveränität versprechen, dieses Versprechen aber häufig nicht einlösen können. Um die Digitale Souveränität der Öffentlichen Verwaltung belastbar zu ermitteln und langfristig zu stärken, braucht es deshalb klar definierte Kriterien, anhand derer Souveränität gemessen wird. Daher hat das ZenDiS auf Grundlage eines Diskussionspapiers („Kriterien zur Bewertung von Digitaler Souveränität – aus messbar wird machbar“) im April 2026 zu einem sechswöchigen Konsultationsprozess eingeladen: Welche Kriterien für Souveränität sollten bewertet werden? Was sind sinnvolle Prüffragen und Nachweise? Wie sollten die verschiedenen Kriterien gewichtet werden? Insgesamt haben wir im Rahmen der Konsultation ca. 70 Rückmeldungen aus Wirtschaft, Verbänden, Wissenschaft, Verwaltung und Zivilgesellschaft erhalten – dafür danken wir allen Beteiligten.¹

Diese Rückmeldungen haben wir sortiert, in rund 20 Themenclustern gebündelt, codiert und ausgewertet. Insgesamt zeigt sich: Unser Vorschlag und die betrachteten Kategorien werden als tragfähige Grundlage gesehen. Hervorgehoben wird insbesondere die organisatorische Perspektive unserer Bewertung, die als wichtiger Unterschied zu bestehenden Rahmenwerken für Cloud-Angebote wie dem EU Cloud Sovereignty Framework (EU CSF) und den Criteria enabling Cloud Computing Autonomy (C3A) des Bundesamts für Sicherheit in der Informationstechnik (BSI) gesehen wird. Kritik- und Diskussionspunkte adressieren im Wesentlichen fünf Themen: 1) eine bessere Berücksichtigung der Gestaltungsfähigkeit der Öffentlichen Verwaltung, 2) eine konkretere Operationalisierung des Frameworks, z. B. anhand überprüfbarer Nachweise, 3) die Frage nach einer möglichen Gewichtung und einem Scoring, 4) die Rolle von Open Source sowie 5) die Konsolidierung mit bestehenden Frameworks (v. a. EU CSF und C3A).

1. Die Rückmeldungen sind öffentlich einsehbar unter https://gitlab.opencode.de/zendis/kriterien-digitale-souveraenitaet/-/work_items.

1. Gestaltungsfähigkeit

Während die Gestaltungsfähigkeit der Öffentlichen Verwaltung im Diskussionspapier als zentrale Dimension benannt wird, bleibt ihre Abbildung im Kriterienkatalog bislang begrenzt. Mehrere Stellungnahmen fordern daher, die Gestaltungsfähigkeit der Organisation als Bewertungsdimension zu stärken. Im Fokus steht dabei die Kooperationsfähigkeit der Verwaltung, sei es bei Open-Source- oder Standardisierungsprojekten oder bei der Zusammenarbeit mit anderen Behörden und Unternehmen: Kann eine Behörde wirksam mit anderen an IT-Lösungen zusammenarbeiten und ihre Bedarfe einbringen?

Unsere Antwort auf diese Rückmeldung

Die Gestaltungsfähigkeit der Organisation wird im ersten Teil der Kriterien nun stärker berücksichtigt. Generell stärken wir unsere Perspektive auf die Organisation als Ganzes, die mehrfach als wichtiges Alleinstellungsmerkmal der ZenDiS-Kriterien genannt wird.

2. Operationalisierung und Nachweise

Ein zweiter Schwerpunkt im Feedback ist die Operationalisierung der Kriterien: Wie wird konkret geprüft, welche Nachweise gelten? Vorgeschlagen wird zudem eine Verschiebung der Nachweise: weg von Absichtserklärungen hin zu tatsächlichen Fähigkeiten. Beteiligte der Konsultation fordern klare Metriken und einfache, aber aussagekräftige Nachweise, die auf Umsetzungstests basieren, nicht nur auf vertraglichen Vereinbarungen. Außerdem wird mehrfach vorgeschlagen, die zeitliche Dimension (z.B. bei einer Migration) zu berücksichtigen, d. h. ein Anbieterwechsel sollte mit vertretbarem Aufwand innerhalb eines angemessenen zeitlichen Rahmens möglich sein. Die Operationalisierung der Kriterien und das Erbringen von Nachweisen müssen dabei insgesamt für die Behörde schlank und umsetzbar bleiben.

Unsere Antwort auf diese Rückmeldung

Die überarbeiteten Kriterien schlagen nun genaue Prüffragen, Antwortskalen und Nachweise vor. Sie folgen damit insgesamt der Logik:

Kategorie → Kriterium → Prüffrage → Antwort → Nachweis → Bewertung.

Auch die zeitliche Dimension wird stärker berücksichtigt. Unser Ansatz basiert weiterhin auf einer Risikobewertung: Businesskritische Anwendungen einer Organisation sollten priorisiert werden. Die Landeshauptstadt München identifiziert in ihrem Souveränitätscheck zunächst die wichtigsten Systemkomponenten anhand des BSI Standards 200-4.² Wir folgen diesem Modell.

2. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html

3. Gewichtung – ja oder nein?

Die Konsultation bestätigt, dass am Ende der Bewertung einer Organisation ein vergleichbares Ergebnis stehen muss bzw. Einzelergebnisse für die betrachteten Bereiche – das „Wie“ ist dabei umstritten: Sollte es eine prozentuale Gewichtung einzelner Kategorien geben, die sich ggf. ausgleichen können, oder harte K.O.-Kriterien? Sollte es einen Score geben oder ein Reifegradmodell?

Unsere Antwort auf diese Rückmeldung

Es muss deutlich werden, in welchen Bereichen der Organisation und ihrer IT-Landschaft kritische Abhängigkeiten mit Handlungsbedarf bestehen. Eine Ausgleichslogik, d.h. ein teilweise mangelhafter Score, der durch einen besseren Score in einer anderen Kategorie ausgeglichen werden kann, schafft Unklarheit im Ergebnis und ermöglicht Souveränitätswashing. Unsere überarbeiteten Kriterien schließen daher an die Gate-Logik der EU-Kommission (EU CSF) an: Es müssen Levels (SEALs) erreicht werden, in der Gesamtbewertung einer Kategorie gilt dann das niedrigste Level, das erreicht wurde. Auf diese Weise erzielen wir eine klare Bewertung und stellen gleichzeitig die europäische Anschlussfähigkeit unserer Kriterien sicher. Wir betrachten die erreichten Level dabei auf Ebene der vorgeschlagenen Kategorien für Souveränität oder einzelner Anwendungen, nicht als Gesamtbewertung einer Organisation, da diese nach Gate-Logik wenig aussagekräftig wäre.

4. Rolle von Open Source

Die Rolle von Open Source für die Digitale Souveränität bildet eine Konfliktlinie in der Konsultation. Die Positionen reichen von Open-Source-Skepsis – hier wird etwa eine mögliche fehlende Kontrolle über Open Source bemängelt oder generell für Technologieoffenheit plädiert – hin zu einer Open-Source-zentrierten Sicht, die Quelloffenheit als notwendige Voraussetzung, wenn auch nicht alleiniges Kriterium, für Digitale Souveränität versteht. Einige Rückmeldungen vertreten eine Governance-orientierte Perspektive: Sie sprechen sich für Open Source aus, gewichten dabei aber Steuerbarkeit und klare Verantwortung bei Open Source mindestens eben so stark wie die reine Verfügbarkeit des Quellcodes.

Unsere Antwort auf diese Rückmeldung

Open Source ist ein wichtiger Hebel für Digitale Souveränität, gerade im Sinne der (Mit-)gestaltungsfähigkeit der Öffentlichen Verwaltung. Voraussetzung ist, dass Open-Source-Software auch weitere Souveränitätsanforderungen – etwa Sicherheit, das Vorhandensein von Support oder die Transparenz der Lieferkette – erfüllt. Open Source sollte nicht auf Kosten anderer Anforderungen an Souveränität bevorzugt werden, doch werden alle Anforderungen von Open-Source- und proprietären Lösungen gleichermaßen erfüllt, sollte Open Source der Vorzug gegeben werden.

5. Konsolidierung mit bestehenden Frameworks (EU CSF und C3A)

Ein weiteres zentrales Feedback der Konsultation betrifft die Konsolidierung der ZenDiS-Kriterien mit bestehenden Referenzrahmen wie dem EU CSF und den C3A.³ Die Rückmeldungen zeigen breite Unterstützung für eine Konsolidierung, allerdings unter Berücksichtigung der besonderen Organisationsperspektive der ZenDiS-Kriterien.

Unsere Antwort auf diese Rückmeldung

Wir sehen einen großen Mehrwert in einer Referenzierung bestehender Rahmenwerke und wollen sicherstellen, dass unsere Kriterien anschlussfähig sind. EU CSF und C3A sind allerdings sehr umfangreich und für viele Behörden schwer zu operationalisieren. Zudem soll das Alleinstellungsmerkmal der ZenDiS-Kriterien – die Organisationsperspektive – erhalten bleiben, allerdings ohne zu einem unverhältnismäßigen Mehraufwand zu führen. Die überarbeiteten ZenDiS-Kriterien referenzieren daher nun die EU-Kriterien. Unser Kriterienkatalog ist dabei als praxisnaher, umsetzbarer Check zu verstehen, der Digitale Souveränität mit überschaubarem Aufwand messbar macht und kritische Abhängigkeiten in der IT-Landschaft systematisch aufdeckt. Zugleich bildet er eine passende Grundlage für eine vertiefte Bewertung nach EU-Kriterien. Ohnehin sehen wir es langfristig nicht als Ziel, dass jede Behörde kritische IT-Lösungen in einem Umfang bewertet, der einer Zertifizierung gleichkommt – die Verwaltung sollte stattdessen zertifizierte Produkte beschaffen können. Diese Entwicklung hin zu zertifizierten Produkten wird auf dem Markt bereits sichtbar. Umso wichtiger wird in Zukunft die Bewertung der Organisation insgesamt sein, mit u. a. ihrer Strategie und Beschaffung, während die Produktbewertung idealerweise an wenigen Stellen erfolgt und dann für alle Behörden verfügbar ist.

3. Seit Juni 2026 liegt außerdem mit dem CADA (Cloud and AI Development Act) der EU eine Unterscheidung von Cloud-Angeboten nach „Union Assurance Level“ vor. Der Act zielt allerdings stärker auf eine Regulierung der Cloud-Anbieter und dient weniger als konkretes Beschaffungs-Framework.

Kriterien und Anwendung

1. Bewertung der organisatorischen Kriterien

Zunächst wird eine Behörde nach organisatorischen Kriterien bewertet. Für jede Prüffrage wird, in Anlehnung an die EU-Kriterien, ein SEAL-Level von 0 bis 4 ermittelt. Es gilt das niedrigste erreichte SEAL-Level (Gate-Logik). Als Nachweis einer digital handlungsfähigen Organisation muss mindestens SEAL-3 erreicht werden.⁴

2. Bewertung der IT-Kriterien

- Im zweiten Schritt werden die eingesetzten IT-Lösungen bewertet. Ausgangspunkt ist die **Kritikalitätsfeststellung** nach dem BSI-Standard 200-4. Auf dieser Grundlage identifiziert eine Behörde die für ihre Aufgabenerfüllung geschäftskritischen Anwendungen.
- Jede dieser Anwendungen wird anschließend anhand der definierten **Prüffragen** bewertet. Die Bewertung erfolgt auf Basis der vorgesehenen Nachweise und führt für jede Prüffrage zu einem SEAL von 0 bis 4. Auch hier gilt die Gate-Logik: Für jede Kategorie ist das niedrigste erreichte SEAL maßgeblich. Da das SEAL auf Ebene der Souveränitätskategorien erfasst wird (Strategische Souveränität, Operative Souveränität, Rechtliche Souveränität, Lieferkettensoeveränität, Souveränität von Daten & KI, Technologische Souveränität), bleiben kritische Bereiche auch auf Anwendungsebene sichtbar.
- **Für geschäftskritische Anwendungen muss mindestens SEAL-3 erreicht werden.** Anwendungen, die dieses Niveau nicht erreichen, weisen in mindestens einem zentralen Souveränitätsaspekt ein Defizit auf und sollten hinsichtlich geeigneter Maßnahmen bewertet werden.

Eine ausführliche Tabelle mit Kriterien, Prüffragen, Nachweisen und SEALs ist angehängt.

4. Erst SEAL-3 ermöglicht „Digitale Resilienz“: EU-Recht ist anwendbar und durchsetzbar, EU-Akteure üben einen wesentlichen, wenn auch nicht vollständigen Einfluss aus, Dienstleistungen, Technologien oder Betriebsabläufe unterliegen lediglich einer marginalen Kontrolle durch Dritte außerhalb der EU. https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf

Kriterienkatalog – Organisation

Kriterien Organisation		
	Organisation	Prüffrage
1	Strategie und Governance	Ist Digitale Souveränität in Strategie, Steuerungsstrukturen und Verantwortlichkeiten der Organisation verbindlich verankert?
2	Beschaffung	Wird Digitale Souveränität verbindlich in Beschaffungs- und Vergabeentscheidungen berücksichtigt?
3	Kollaboration	Ist die Organisation in der Lage, an digitalen Lösungen mit anderen Organisationen, Herstellern oder Communities zusammenzuarbeiten und eigene Anforderungen wirksam einzubringen?
4	Risikomanagement	Werden Abhängigkeiten auf Basis einer Risikoanalyse systematisch identifiziert und gesteuert?
5	Auftrageberfähigkeit	Ist die Organisation in der Lage, Anforderungen zu formulieren, Angebote zu bewerten und Anbieter wirksam zu steuern?
6	Kompetenzen	Verfügt die Organisation über ausreichende interne IT-Kompetenzen, um ihre IT fachlich zu beurteilen, Entscheidungen zu treffen und notwendige Veränderungen wirksam zu steuern?
7	Compliance Management	Werden regulatorische und organisatorische Anforderungen (z. B. DSGVO) kontinuierlich überwacht und eingehalten?
8	Modularität der IT-Landschaft	Sind die zentralen IT-Systeme der Behörde modular aufgebaut und so integriert, dass einzelne Komponenten austauschbar sind, ohne das Gesamtsystem wesentlich zu beeinträchtigen?

Kriterienkatalog – IT

Kriterien IT			
	Kriterium	Referenz	Prüffrage
1	Resilienz gegen- über Abschaltung	<i>EU CSF SOV-1.8</i>	Kann der Dienst auch bei Wegfall des Herstellers oder zentraler Zulieferer weiter betrieben werden?
2	Rechtshoheit	<i>EU CSF SOV-2.3</i>	Liegt die alleinige rechtliche und tatsächliche Kontrolle über die Lösung bei juristischen Personen mit Sitz in der EU oder im EWR?
3	Schlüsselkontrolle	<i>EU CSF SOV-3.1</i>	Verfügt die Behörde über die ausschließliche Kontrolle kryptographischer Schlüssel?
4	Datenlokation	<i>EU CSF SOV-3.4</i>	Wo werden Daten gespeichert und verarbeitet und in welchem Umfang kann dies kontrolliert werden?
5	KI	<i>EU CSF SOV-3.5</i>	Werden Modelle eingesetzter KI, Trainingsdaten und KI-Infrastrukturen unter europäischer Kontrolle transparent entwickelt, betrieben und bereitgestellt?
6	Portabilität und Interoperabilität	<i>EU CSF SOV-4.1</i>	Können Daten und Workloads innerhalb von 30 Tagen verlustfrei auf alternative Lösungen oder Anbieter übertragen werden?
7	Dokumentation und Wissenstransfer	<i>EU CSF SOV-4.5</i>	Sind Dokumentation und Betriebswissen vollständig verfügbar, um langfristige Unabhängigkeit sicherzustellen?
8	Souveränität von Unterauftragnehmern	<i>EU CSF SOV-4.6</i>	Können Betrieb, Wartung, Support und Migration durch mehrere voneinander unabhängige Anbieter erbracht werden, ohne dass die Architektur einen bestimmten Anbieter voraussetzt?
9	Herkunft der Software	<i>EU CSF SOV-5.4</i>	Wie transparent ist die Herkunft der Software und ihrer wesentlichen Komponenten, und in welchem Umfang stammen diese aus der EU?
10	Technologische Abhängigkeit	<i>EU CSF SOV-5.6</i>	Besteht eine Abhängigkeit von nicht-EU-Anbietern, -Infrastrukturen oder proprietären Technologien?
11	Transparenz der Lieferkette	<i>EU CSF SOV-5.7</i>	Ist die Lieferkette einschließlich Unterauftragnehmern vollständig transparent und auditierbar?
12	Offene Standards und Schnittstellen	<i>EU CSF SOV-6.1</i>	Nutzt die Lösung offene, dokumentierte Standards und standardisierte Schnittstellen zur Integration mit anderen Systemen?
13	Verfügbarkeit von Open Source	<i>EU CSF SOV-6.3</i>	Ist die Software unter offenen Lizenzbedingungen verfügbar, die Nutzung, Prüfung, Anpassung und Weitergabe ermöglichen?

Strategische Souveränität	Operative Souveränität
Rechtliche Souveränität	Lieferkettensoveränität
Souveränität von Daten & KI	Technologische Souveränität

Über das ZenDiS

Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) unterstützt die Öffentliche Verwaltung in Bund, Ländern und Kommunen dabei, sich aus kritischen Abhängigkeiten von einzelnen Technologieanbietern zu lösen. Dazu stellt es neben Kompetenzen, Services und Beratung auch eine Kooperations- und Entwicklungsplattform sowie leistungsfähige, skalierbare und leicht zugängliche Open-Source-Lösungen bereit. Zudem bündelt das ZenDiS die Anforderungen der Öffentlichen Verwaltung und stellt gemeinsam mit seinen Partnern sicher, dass Lösungen bedarfsgerecht weiterentwickelt und zuverlässig betrieben werden.

Herausgeber

Zentrum für Digitale Souveränität der Öffentlichen Verwaltung GmbH (ZenDiS)
Suttner-Nobel-Allee 4
44803 Bochum

E-Mail: hallo@zendis.de

Web: www.zendis.de

Ansprechpartnerin

Dr. Lea Beiermann
Partnership Lead
lea.beiermann@zendis.de

Stand

Oktober 2026

