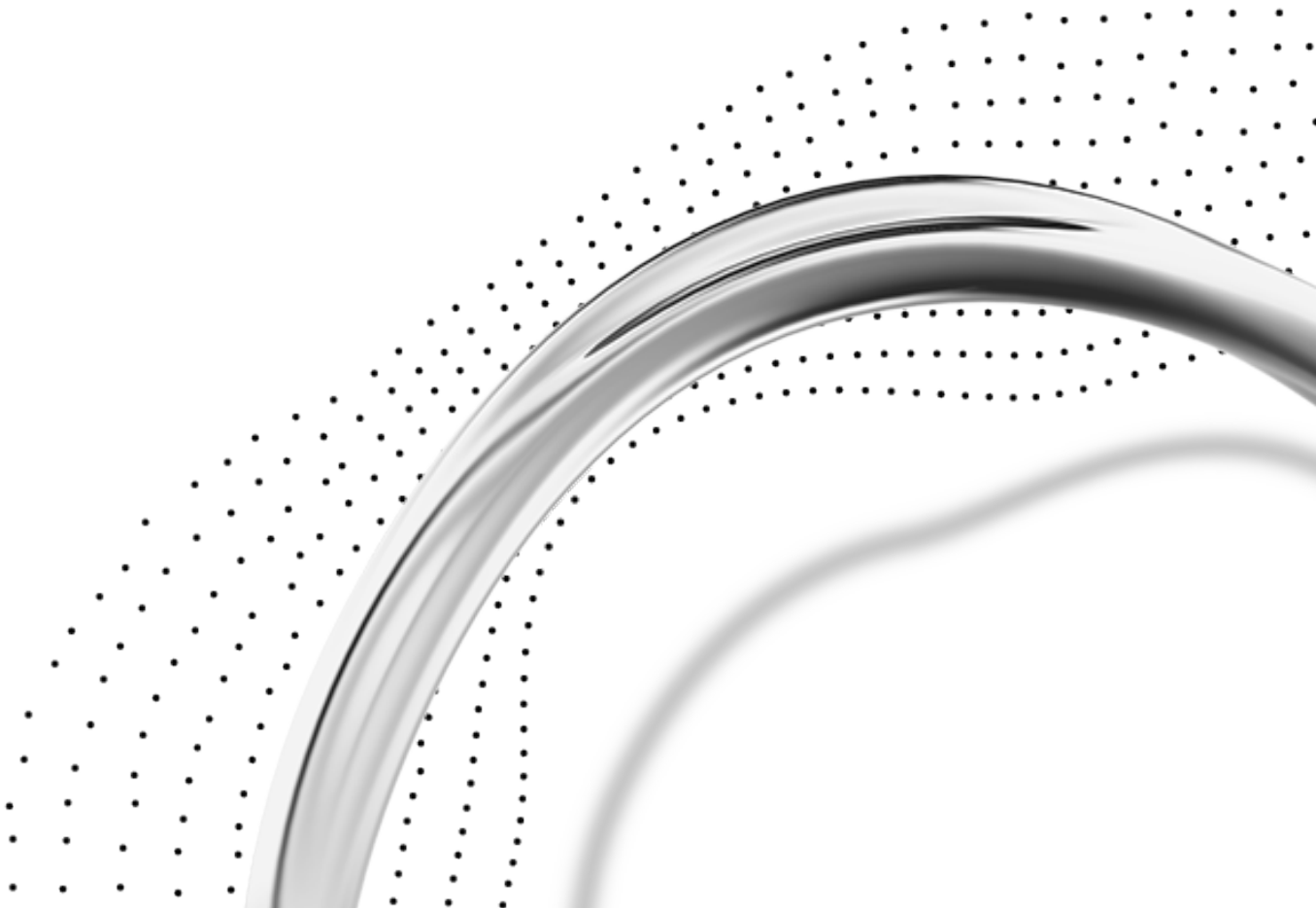
Diskussionspapier

Kriterien zur Bewertung von Digitaler Souveränität

— aus messbar wird machbar



Inhalt

Executive Summary

Die Verfügbarkeit digitaler Dienste und Technologien ist für die Öffentliche Verwaltung (ÖV) lebensnotwendig. Diese Verfügbarkeit kann durch äußere Faktoren, wie zum Beispiel politische Einflussnahme oder technologische Abhängigkeiten, eingeschränkt werden. Es liegt in der Verantwortung der ÖV, für einen stabilen und sicheren Betrieb ihrer Informationstechnologie (IT) zu sorgen.

Aus dieser Notwendigkeit heraus wurde die „Digitale Souveränität der Öffentlichen Verwaltung“ durch den IT-Planungsrat (IT-PLR) als Leitbegriff definiert und durch strategische Ziele konkretisiert.[1]

Diese Ziele lassen sich in einen Katalog konkreter Prüfkriterien überführen, die einen systematischen Souveränitätscheck von IT-Lösungen und Infrastrukturen bis hin zu ganzen Behörden (Prozesse, Strukturen etc.) ermöglichen.

Der hier vorgeschlagene Kriterienkatalog basiert auf den strategischen Zielen des IT-PLR und wird bis Mitte Mai 2026 im Rahmen eines offenen Konsultationsprozesses mit openCode weiterentwickelt.

Direkt am Konsultationsprozess mit openCode teilnehmen:

www.souveränitätscheck.de

1. Bundesministerium des Innern, für Bau und Heimat (BMI). (2021, Januar). Beschluss 2021/09: Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung. Berlin. IT Planungsrat. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf , zuletzt abgerufen am 19.03.2026.

1. Digitale Souveränität ist entscheidend

„Digitale Souveränität“ bezeichnet die Fähigkeit von Organisationen – wie auch von Individuen und Staaten – ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.[2] Entscheidungen und Handlungen sollten jederzeit rechtskonform, sicher, nachhaltig und wirtschaftlich tragfähig zu gestalten und umzusetzen sein.

Dazu gehören die bewusste Steuerung von Abhängigkeiten sowie die Sicherung von Reversibilität (Exit-Fähigkeit) wesentlicher digitaler Komponenten.[3] Die Digitale Souveränität der Öffentlichen Verwaltung ist damit keine technische Nischenfrage, sondern Voraussetzung für Rechtsstaatlichkeit, Daseinsvorsorge und demokratische Resilienz im 21. Jahrhundert.

Die Kontrolle über die öffentliche digitale Infrastruktur liegt aktuell jedoch nicht bei der öffentlichen Hand. Damit ist ihre Handlungsfähigkeit langfristig gefährdet und schon jetzt eingeschränkt: Eine Umfrage der Kommunalen Gemeinschaftsstelle für Verwaltungsmanagement (KGSt) ergab 2020, dass 87 Prozent der befragten Kommunen sich als ganz oder teilweise abhängig von einzelnen Software- und Cloudanbietern betrachten.[4]

Im „Tech Stack“[5] der deutschen Bundesbehörden und der IT-Dienstleister der öffentlichen Hand findet man nahezu überall die gleichen Anwendungen von wenigen – meist US-amerikanischen – Anbietern. Das gilt für alle Schichten des Stacks, vor allem aber für Büro-Software, Arbeitsplatz- und Server-Betriebssysteme. Einer Marktanalyse von 2019 zufolge verwenden in diesen Bereichen 96 Prozent aller unmittelbaren Bundesbehörden die Software nur eines Anbieters.[6]

2. „Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung; Eckpunkte – Ziel und Handlungsfelder“ (Beschluss in der 31. Sitzung des IT-PLR, Entscheidung 2020/07 sowie Beschluss im IT-Rat Nr. 2020/01).
3. Goldacker, G. (2017). Digitale Souveränität – Was genau ist Digitale Souveränität? Fraunhofer-Institut FOKUS, Kompetenzzentrum Öffentliche IT (ÖFIT). https://publica.fraunhofer.de/entities/publication/8a0846aa-ec67-4788-8f0b-4bb540d97162, zuletzt abgerufen am 19.03.2026; Mohabbat Kar, R., und Thapa, B. E. P. (2020). Digitale Souveränität als strategische Autonomie – Umgang mit Abhängigkeiten im digitalen Staat (Weißbuch); Fraunhofer-Institut FOKUS, Kompetenzzentrum Öffentliche IT (ÖFIT). https://publica.fraunhofer.de/entities/publication/67656462-b94f-499b-ad44-b2cc1834dec3, zuletzt abgerufen am 19.03.2026.
4. Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (KGSt). (2020, Mai). Open Source in Kommunen: Ergebnisse einer Umfrage (KGSt Denkanstoß). Köln. https://www.kgst.de/documents/20181/34177/2020_Denkanstoss_Open+Source+in+Kommunen_Umfrage.pdf/22fd4755-0418-9f98-b69d-5cd3b845a477, zuletzt abgerufen am 19.03.2026.
5. Kombination der Technologiekomponenten, welche zur Erstellung von IT-Anwendungen und -Infrastrukturen verwendet werden.
6. PwC Strategy& (Germany) GmbH. (2019). Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern: Eine Studie im Auftrag des Bundesministeriums des Innern, für Bau und Heimat. Berlin. https://wibe.de/wp-content/uploads/20190919_strategische_marktanalyse-compressed.pdf, zuletzt abgerufen am 19.03.2026.

Die IT-Landschaft der Öffentlichen Verwaltung ist eine Monokultur – und das birgt Risiken: [7]

+ **Datenschutzrechtliche Unsicherheiten**
durch exterritoriale Rechtszugriffe auf Daten

+ **Eingeschränkte Informationssicherheit**
durch fehlende Kontrolle über Code und Daten

+ **Inflexibilität**
durch fehlende Wechseloptionen und technologischen Lock-in

+ **Unkontrollierbare Kosten**
aufgrund steigender Lizenzgebühren für cloudbasierte SaaS-Modelle

+ **Fremdgesteuerte Innovation**
durch Abhängigkeit von proprietären Entwicklungszyklen[8] globaler Anbieter

Diese Risiken werden durch aktuelle technische und geopolitische Entwicklungen verstärkt: Der Trend zu cloudbasierten Software-as-a-Service-Lösungen im Abonnement erlaubt weniger Kontrolle über Code und Daten und wird begleitet von steigenden Lizenzkosten.[9] Hinzu kommt eine neue Unberechenbarkeit in den transatlantischen Beziehungen: Eine gezielte Einflussnahme der US-amerikanischen Politik auf öffentliche europäische IT-Infrastruktur ist nicht länger ausgeschlossen. Die Debatte um den gesperrten E-Mail-Account von Karim Khan, Chefankläger des Internationalen Strafgerichtshofs, verdeutlichte dieses Risiko im Mai 2025.[10]

7. Ibid.
8. Proprietäre Entwicklungszyklen meint hier Entwicklungszyklen, die durch einen Technologieanbieter ohne Einflussmöglichkeit der Nutzerinnen und Nutzer bzw. Kunden gesteuert werden.
9. Kirlidokme, B. (2025, 21. Februar). Bundesregierung gibt mehr als eine Milliarde für Software aus – US Tech Konzerne profitieren. Frankfurter Rundschau. https://www.fr.de/wirtschaft/bundesregierung-gibt-mehr-als-eine-milliarde-fuer-software-aus-93586564.html, zuletzt abgerufen am 19.03.2026.
10. Laaff, M. (2025, 23. Juli). Diese E-Mail ist unzustellbar: Was, wenn Donald Trump Big Tech zwingt, die Dienste in Europa abzuschalten? Lange war das Theorie. Dann ging eine wichtige Mailadresse am Strafgerichtshof nicht mehr. Die Zeit. https://www.zeit.de/digital/internet/2025-07/microsoft-email-sperre-karim-khan-donald-trump-istgh, zuletzt abgerufen am 19.03.2026.

2. Digitale Souveränität messbar machen – aus messbar wird machbar

Der politische und öffentliche Diskurs zur Digitalen Souveränität nimmt zu. Auch internationale Hyperscaler bedienen sich des Begriffs, um ihren Kunden zu versichern, dass in der Public Cloud keine Bedenken hinsichtlich ihrer Souveränität – beispielsweise IT-Sicherheit und Datenschutz – bestehen. Serverstandorte in der EU, air-gapped oder Confidential Clouds sollen Digitale Souveränität garantieren. Dabei wird häufig außer Acht gelassen, dass der Rechtsstandort ausländischer Unternehmen einen Zugriff auf IT-Infrastruktur auch in der EU im Prinzip zulässt. Digitale Souveränität droht zu einem reinen Marketingbegriff zu werden.

Gleichzeitig fehlt eine belastbare Grundlage, um zu bewerten, wie digital souverän die Öffentliche Verwaltung heute ist. Mit dem Cloud Sovereignty Framework der Europäischen Union (EU) gibt es erste Kriterien, um Cloud-Angebote zu bewerten. Auf deren Grundlage entwickelt das Bundesamt für Sicherheit in der Informationstechnik (BSI) nun allgemeine Souveränitätskriterien für Cloud-Lösungen. Jedoch gibt es keine belastbaren Kriterien für die Digitale Souveränität der ÖV insgesamt.[11] Die Digitale Souveränität der ÖV kann derzeit weder valide eingeschätzt noch verglichen oder gesteuert werden.

Daher braucht es klar definierte Kriterien, anhand derer Digitale Souveränität gemessen werden kann. Es geht dabei nicht nur um die (Un-)Abhängigkeit einzelner Software-Lösungen, sondern um die Handlungsfähigkeit öffentlicher Einrichtungen insgesamt – inklusive ihrer gesamten IT-Infrastruktur und den darauf aufbauenden digitalen Diensten. Nur so wird Souveränität für die Verwaltung messbar und machbar, denn: „You can't manage what you can't measure."

Messbarkeit ermöglicht:

- Identifikation kritischer Abhängigkeiten
- Strategische Investitionssteuerung
- Nachweis souveräner IT im Sinne von Compliance, Sicherheit und Resilienz
- Vergleichbarkeit zwischen Behörden
- Perspektivisch eine Darstellung der Entwicklung Digitaler Souveränität der ÖV

11. European Commission. (2025, October). Cloud Sovereignty Framework (Version 1.2.1). Luxembourg: European Commission. https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?filename=Cloud-Sovereignty-Framework.pdf, zuletzt abgerufen am 19.03.2026.

Beispiele für bestehende Abhängigkeiten

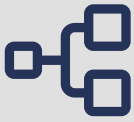
Beispiel Cloud

Die Frage der Digitalen Souveränität bei Cloud-Diensten ist seit Jahren politisch relevant. 2019 wurde im Rahmen von Gaia-X das Projekt Sovereign Cloud Stack (SCS)[12] gestartet, gefördert zunächst durch die Bundesagentur für Sprunginnovationen (SPRIND) und bis Ende 2024 durch das Bundesministerium für Wirtschaft und Energie (BMWE). Das Ziel war, mit offenen Standards und Schnittstellen eine größtmögliche Unabhängigkeit von proprietären Technologien und Produkten im Cloud-Betrieb zu schaffen.

2020 legten die Föderale IT-Kommission (FITKO) und das Bundesministerium des Innern (BMI) in der Strategie für die Deutsche Verwaltungscloud die Wechselmöglichkeit zwischen Anbietern als zentrales Kriterium fest. 2023 veröffentlichte die Datenschutzkonferenz (DSK) ein Positionspapier[13] mit Anforderungen an eine souveräne Cloud-Nutzung: volle Kontrolle über Daten, transparente technische Prozesse und die Möglichkeit zum Anbieterwechsel oder Eigenbetrieb. Ohne diese Bedingungen sieht die DSK Cloud-Lösungen nicht als rechtskonform an.

12. Siehe auch: https://gaia-x.eu/ und https://scs.community/de/
13. Vgl. https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf, zuletzt abgerufen am 19.03.2026.

Beispiele für bestehende Abhängigkeiten



Beispiel KI

Bei Diensten auf Basis von künstlicher Intelligenz (KI) ist schwer nachzuvollziehen, wie die eingesetzten Modelle trainiert wurden und wie ihre Ergebnisse zustande kommen. Open Weight Models (OWM) legen zwar die Modellparameter offen, selten jedoch die verwendeten Trainingsdaten. Die weit verbreiteten Closed Source Models (CSM) wiederum agieren als vollständige „Blackbox".

Auch nutzen Anbieter von CSM oft User-Anfragen (Prompts, hochgeladene Dateien, User-Feedback und Interaktionen), um ihre Modelle nachzutrainieren und Dienste weiterzuentwickeln – dazu werden diese Anfragen oftmals von den Anbietern gespeichert und für nachfolgende Anfragen genutzt. Dies kann dazu führen, dass selbst die Inhalte dieser vorherigen Anfragen anderen Nutzenden zugänglich gemacht werden und somit ausreichende Datensicherheit nicht gewährleistet ist.

Die Stärkung souveräner KI-Technologien in Deutschland und Europa wurde im Rahmen der Deutschen Ministerpräsidentenkonferenz (MPK) als strategisches Kernziel identifiziert.[14] Die Entwicklung souveräner KI-Anwendungen erfordert modulare Software-Architekturen mit standardisierten Schnittstellen, eine möglichst unabhängige Betriebsinfrastruktur und einen verantwortungsvollen Umgang mit User-Daten.

Open-Source-KI, insbesondere OWM, bietet hier die Möglichkeit, Abhängigkeiten zu reduzieren und die vollständige Kontrolle über Daten und Anwendungen zu gewährleisten. Sie erfordert jedoch eine aktive Community, eine professionelle Governance und entsprechende Betreiber-Expertise, um langfristige Wartbarkeit und Weiterentwicklung von Anwendungen sicherzustellen.

14. Konferenz der Regierungschefinnen und Regierungschefs der Länder. (2025, März). Beschluss TOP 2: Technologische Souveränität sichern – KI-Standorte Europa und Deutschland stärken. Berlin. https://www.ministerpraesident.sachsen.de/ministerpraesident/07_TOP2_Beschluss_MPK_RS.pdf, zuletzt abgerufen am 19.03.2026.

3. Von Prinzipien zu Parametern: Kriterienkatalog

Der IT-PLR entwickelte infolge der Analyse des „Tech Stacks“ der ÖV von 2019 eine Strategie, um die Handlungsfähigkeit der Verwaltung nachhaltig zu sichern. Der Kern der Strategie ist die Stärkung der Digitalen Souveränität in drei Dimensionen: Wechselmöglichkeit, Gestaltungsfähigkeit und Einflussnahme.[15]

Die Öffentliche Verwaltung soll in der Lage sein, IT-Lösungen, Komponenten und Anbieter flexibel auszuwählen und bei Bedarf mit vertretbarem Aufwand zu wechseln. Sie soll außerdem ihre IT mitgestalten können, wozu entsprechende Fachkompetenzen und geeignete Kooperationsstrukturen einerseits und gestaltbare, offene Technologien andererseits erforderlich sind. Zudem muss die ÖV ihre Anforderungen gegenüber Technologieanbietern wirksam vertreten können, etwa wenn es um Vertragsbedingungen, Sicherheitsstandards oder den Betrieb im eigenen Rechenzentrum geht.

Ausgehend von diesen strategischen Zielen für die Digitale Souveränität lassen sich konkrete Kriterien ableiten, mit denen die Digitale Souveränität von Behörden und Organisationen systematisch bewertet werden kann.

15. Bundesministerium des Innern, für Bau und Heimat (BMI). (2021, Januar). Beschluss 2021/09: Strategie zur Stärkung der digitalen Souveränität für die IT der öffentlichen Verwaltung. Berlin. IT Planungsrat. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf, zuletzt abgerufen am 19.03.2026.

3. Von Prinzipien zu Parametern: Kriterienkatalog

A. Organisation und Fähigkeiten

Der Fokus dieser Kategorie liegt auf der Management- und Steuerungsfähigkeit einer Organisation hinsichtlich der Risiken und der Erfüllung der Anforderungen an digital souveräne Dienste. Bewertet wird, ob die Digitale Souveränität als strategisches Ziel verankert ist und ob die Organisation über die notwendigen Fähigkeiten verfügt, Einfluss auf Technologieanbieter zu nehmen und souveräne Entscheidungen zu treffen.

- Strategie (Existenz und Wirksamkeit einer souveränitätsorientierten Digitalstrategie)
- IT-Governance & Management
- Risikomanagement
- Beschaffung und Vergabe
- Auftraggeberfähigkeit
- Kompetenzen als Voraussetzung der Einflussnahme auf Anbieter

Diese Dimension adressiert die Kernfrage:
Ist die Organisation überhaupt in der Lage, Digitale Souveränität aktiv zu steuern?

3. Von Prinzipien zu Parametern: Kriterienkatalog

B. Digitale Anwendungen und Dienste

Diese Kategorie bewertet die Gestalt- und Austauschbarkeit der genutzten Anwendungen sowie Kontrolle über diese Anwendungen. Im Zentrum steht die Frage, inwieweit digitale Dienste modular, transparent und interoperabel gestaltet sind und ob ihre Nutzung die Wechselmöglichkeit (Exit-Fähigkeit) gewährleistet. Geprüft werden folgende Bereiche:

- Transparenz und Dokumentation
- Nachvollziehbarkeit und Sicherheit der Lieferkette
- Anwendungsarchitektur und Modularität
- Standards und Schnittstellen
- Abhängigkeiten auf Software-Ebene

Hier geht es um die Frage:
Ermöglichen die eingesetzten Anwendungen technologische Selbstbestimmung – oder führen sie zu Abhängigkeiten, die die Handlungsfähigkeiten einschränken?

3. Von Prinzipien zu Parametern: Kriterienkatalog

C. Informationen und Daten

Diese Kategorie überprüft, inwieweit Datenhoheit und Datensouveränität gewährleistet sind. Der Fokus liegt auf regulatorischen, technischen und betrieblichen Bedingungen, die den souveränen Umgang mit Daten ermöglichen. Betrachtete Bereiche sind:

- Datenlokation
- Datensicherheit
- Datenschutz
- Datenstrukturen

Bewertet wird, ob

Behörden jederzeit die volle Kontrolle über ihre Daten ausüben können – einschließlich Zugriff, Speicherung, Verarbeitung, Löschung und Migration.

3. Von Prinzipien zu Parametern: Kriterienkatalog

D. Betrieb und Infrastruktur

Diese Kategorie bewertet die technische und organisatorische Betriebssouveränität. Im Mittelpunkt stehen die Unabhängigkeit im Betrieb, die Resilienz gegenüber externen Einflüssen und die Fähigkeit zum Anbieterwechsel. Betrachtet werden:

- Abhängigkeit auf Betriebs- bzw. Provider-Ebene
- Kundenverhältnis
- Exit-Fähigkeit
- Resilienz und Business Continuity
- Sicherheit und Compliance im Betrieb

Diese Dimension beantwortet die Frage:
Kann die Verwaltung ihre Systeme dauerhaft, sicher und unabhängig betreiben, auch bei exogenen Störungen oder geopolitischen Spannungen?

4. Eine risikobasierte Anwendung der Kriterien

Nicht jede IT-Komponente bringt dieselben Risiken mit sich. Daher ist eine risikobasierte Bewertung notwendig, um Digitale Souveränität, Wirtschaftlichkeit und praktische Umsetzbarkeit sicherzustellen. Die Tiefe und Priorität der Bewertung richten sich insbesondere nach:[16]

+ Datenkritikalität:
Anforderungen hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit der durch die IT-Infrastruktur verarbeiteten Daten.

+ Sicherheitslage:
Technische und organisatorische Schutzmaßnahmen, Schwachstellenexposition und Reifegrad der Sicherheitskontrollen.

+ Rechtsrisiko:
Regulatorische Anforderungen, die erfüllt werden müssen, zum Beispiel Datenschutz, Transfers, Branchenrecht oder Vorgaben wie NIS2, CRA und AI-Act.

+ Verwaltungsprozesse:
Art, Umfang und Kritikalität der Verwaltungsprozesse, die auf die IT-Infrastruktur der Organisation angewiesen sind.

+ Abhängigkeitsgrad:
Abhängigkeit von einzelnen Anbietern, proprietären Lösungen sowie Machbarkeit einer Datenrückmigration, um Lock-in-Effekte zu vermeiden.

+ Lieferkettenzuverlässigkeit:
Stabilität und Integrität der Lieferkette einschließlich Einhaltung rechtlicher Vorgaben wie der Vergabeverordnung oder dem Lieferkettensorgfaltspflichtengesetz.

16. Bundesministerium des Innern und für Heimat. (2024). Anforderungen an Technologieanbieter und -lösungen (Beschluss Nr. 2024/01).

5. Souveränitätscheck

Die definierten Kategorien, Kriterien und Risikoaspekte bilden die Grundlage für einen praxisnahen Souveränitätscheck auf der Ebene einzelner Behörden mit ihrer jeweiligen IT-Infrastruktur: Jedes Kriterium kann durch Prüffragen operationalisiert werden, die es ermöglichen, die Digitale Souveränität systematisch zu bewerten. Zudem können Nachweise und Audit-Methoden definiert werden – wie Dokumentation, Richtlinien, technische Prüfberichte oder Zertifizierungen. So können Behörden erkennen, welche Anforderungen erfüllt sind und wo Handlungsbedarf besteht, um ihre Digitale Souveränität zu stärken.

Der Souveränitätscheck wird – ausgehend von den vorgeschlagenen Kategorien und Kriterien – in einem offenen Konsultationsprozess mit der Plattform openCode des Zentrum für Digitale Souveränität der Öffentlichen Verwaltung entwickelt. Der Kriterienkatalog wird bis Mitte Mai 2026 gemeinsam diskutiert, geprüft und weiterentwickelt. So entsteht ein praxisfähiges, flexibel anwendbares Instrument zur Bewertung der Digitalen Souveränität, das durch die Konsultation zudem auf einer breiten Basis steht und Verbindlichkeit schafft.

Direkt am Konsultationsprozess mit openCode teilnehmen:

www.souveränitätscheck.de

Anlage

Kriterien zur Messung Digitaler Souveränität

Strategische Ziele

- **Gestaltungsfähigkeit** = Fähigkeit, IT-Infrastruktur und digitale Dienste aktiv mitzugestalten und nach Bedarf anzupassen
- **Wechselmöglichkeit** = Möglichkeit, IT-Lösungen, Komponenten und Anbieter flexibel auszuwählen und bei Bedarf mit vertretbarem Aufwand zu wechseln
- **Einflussnahme auf IT-Anbieter** = Fähigkeit, Anforderungen gegenüber Technologieanbietern wirksam zu vertreten

Kriterien zur Messung Digitaler Souveränität			
A	**Organisation und Fähigkeiten**		**Ziel**
A1	**Strategie**	Ist Digitale Souveränität in der Digitalstrategie und den übergeordneten Leitlinien der Organisation verankert?	● ◆
A2	**IT-Governance & Management**	Sind Verantwortlichkeiten, Prozesse und Steuerungsstrukturen im IT-Betrieb definiert und umgesetzt?	● ◆
A3	**Risikomanage-ment**	Werden technologische, organisatorische und strategische Risiken im Hinblick auf Abhängigkeiten erfasst und gesteuert?	● ■ ◆
A4	**Beschaffung und Vergabe**	Werden Beschaffungsprozesse so gestaltet, dass Wettbewerb, Offenheit und Alternativen berücksichtigt werden?	● ■ ◆
A5	**Auftraggeber-fähigkeit**	Ist die Organisation in der Lage, IT-Projekte eigenständig zu steuern und Anbieter wirksam zu kontrollieren?	● ◆
A6	**Kompetenzen**	Verfügt die Organisation über die nötigen (IT-)Kenntnisse, Fachkräfte und Wissensbestände, um souverän handeln zu können?	● ■ ◆
B	**Digitale Anwendungen und Dienste**		**Ziel**
B1	**Transparenz/ Dokumentation**	Ist eine umfassende Dokumentation von Anwendungen hinsichtlich der Funktionalität, der Schnittstellen und der Datenstrukturen sowie des Zusammenspiels der Komponenten im Systemkontext mit anderen Anwendungen oder Diensten zum Zwecke der Nutzung, Auditierung, der Wartung und der Inbetriebnahme vorhanden?	● ■
B2	**Nachvollziehbarkeit und Sicherheit der Lieferkette**	Ist die Herkunft von Hardware- und Software-Komponenten der Organisation – einschließlich Herstellungsorte, beteiligter Länder, Anbieter außerhalb der EU und Transparenz der gesamten Lieferkette – bekannt und überprüfbar?	● ■
B3	**Anwendungs-architektur/ Modularität**	Sind Anwendungen portabel und modular aufgebaut und technisch entkoppelbar?	● ■
B4	**Standards**	Nutzen Anwendungen offene Schnittstellen und etablierte Standards, um Austauschbarkeit und Integration zu ermöglichen?	● ■
B5	**Abhängigkeit auf Software-Ebene**	In welchem Umfang bestehen Lock-in-Risiken durch proprietäre Software oder fehlende Alternativen?	■ ◆

Kriterien zur Messung Digitaler Souveränität			
C	**Daten**		**Ziel**
C1	**Datenlokation**	Wo werden Daten gespeichert und verarbeitet (lokal, EU, Drittstaaten) und wie ist dies zu kontrollieren?	■ ◆
C2	**Datensicherheit**	Werden Daten umfassend verschlüsselt und gibt es entsprechende Konzepte sowie technische und organisatorische Maßnahmen, welche die Datensicherheit Ende-zu-Ende gewährleisten?	●
C3	**Datenschutz**	Werden rechtliche Vorgaben (z. B. DSGVO) eingehalten und durch technische sowie organisatorische Maßnahmen abgesichert?	● ◆
C4	**Datenstrukturen**	Sind Daten in offenen, interoperablen Formaten abgelegt, sodass Portabilität und Wiederverwendbarkeit gesichert sind?	● ■
D	**Betrieb und Infrastruktur**		**Ziel**
D1	**Abhängigkeit auf Betriebs-/ Provider-Ebene**	Wie stark ist die Bindung an einzelne Betreiber, Dienstleister oder Cloud-Anbieter und sind diese durch EU-Recht kontrollierbar?	■ ◆
D2	**Kundenverhältnis**	Erlaubt das Kundenverhältnis eine Einflussnahme auf Software-Entwicklung und digitale Dienste, beispielsweise durch eine transparente Release-Planung und aktivem Anforderungsmanagement?	● ◆
D3	**Exit-Fähigkeit**	Ist ein Anbieterwechsel oder Rückführung in Eigenbetrieb realistisch und erprobt?	■
D4	**Resilienz & Business Continuity**	Wie robust sind die Systeme gegenüber Ausfällen, Krisen oder Angriffen und wie schnell ist ein Wiederanlauf möglich?	●
D5	**Sicherheit und Compliance im Betrieb**	Werden regulatorische und organisatorische (EU-)Anforderungen im laufenden Betrieb durchgängig überprüft und eingehalten?	● ◆

Über das ZenDiS

Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) wurde 2022 vom Bund gegründet. Als Kompetenz- und Servicezentrum unterstützt das ZenDiS die Öffentliche Verwaltung im Bund, in den Ländern und Kommunen dabei, ihre Handlungsfähigkeit im digitalen Raum langfristig abzusichern – vor allem, indem kritische Abhängigkeiten von einzelnen Technologieanbietern aufgelöst werden. Dazu konzentriert sich das ZenDiS in der ersten Ausbaustufe darauf, den Einsatz von Open-Source-Software in der Öffentlichen Verwaltung voranzutreiben. Das ZenDiS ist eine GmbH und liegt derzeit zu 100 Prozent in der Hand des Bundes. Die Beteiligungsführung liegt beim Bundesministerium für Digitales und Staatsmodernisierung (BMDS). Sitz des ZenDiS ist Bochum.

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

Ansprechpartner
Lutz Niemeyer | Kommunikation |
lutz.niemeyer@zendis.de

Stand
März 2026