VITAKO

POSITION

# DIGITALE SOUVERÄNITÄT:

Handlungsfähigkeit sichern, Entscheidungsfreiheit ermöglichen

VITAKO–Positionspapier

Stand 26.10.2026

## Das Wichtigste in Kürze

Die öffentliche Verwaltung in Deutschland hängt in weiten Teilen von wenigen nicht-europäischen Anbietern ab – bei Soft- und Hardware, bei Cloud-Diensten und bei Künstlicher Intelligenz. Diese Abhängigkeit macht den Staat erpressbar, belastet mit hohen Lizenzzahlungen zunehmend die öffentlichen Haushalte und wirft datenschutzrechtliche Fragen auf.

Unsere Position: Digitale Souveränität sichert die Handlungsfähigkeit des Staates. Sie ist Voraussetzung dafür, dass die Verwaltung auch künftig zuverlässig funktioniert – und nicht vom Ermessen anderer Regierungen abhängig ist. Es gilt, den Verwaltungen Entscheidungsfreiheit zu ermöglichen. Souveränität heißt nicht Verzicht auf proprietäre Produkte, sondern die Fähigkeit, zu wählen und zu wechseln.

Vor diesem Hintergrund empfiehlt VITAKO folgende Schritte auf dem Weg zu mehr digitaler Souveränität in der Verwaltung:

- Eine koordinierte Gesamtstrategie mit konkreten Meilensteinen, klaren Zuständigkeiten und messbaren Indikatoren bis zum Ende der Legislatur vorlegen.
- Öffentliche Beschaffung strategisch nutzen und gebündelte Aufträge für heimische und europäische Anbieter einsetzen – auch zugunsten der Kommunen.
- Offene Standards verbindlich einfordern und den EU Data Act konsequent durchsetzen.
- Souveräne Infrastruktur bereitstellen, die Deutsche Verwaltungscloud als zentralen Baustein nutzen und den Deutschland-Stack dauerhaft finanzieren.
- Interoperabilität ermöglichen, indem die öffentliche Hand für alle relevanten IT-Produkte offene Standards vorschreibt.
- CyberGovSecure auf die kommunale Ebene ausweiten, einschließlich anteiliger Finanzierung.

## 1. Warum jetzt? Der Handlungsdruck steigt.

Im Frühjahr 2025 verlor der Chefankläger des Internationalen Strafgerichtshofs (IStGH) in Den Haag den Zugang zu seinem E-Mail-Konto. Keine technische Panne, sondern eine politische Entscheidung: Die US-Regierung hatte Sanktionen gegen ihn verhängt, und sein Postfach lag bei einem US-Anbieter. Was jahrelang als überzogenes Szenario abgetan wurde, ist damit eingetreten – ein Behördenzugang wurde abgeschaltet, weil ein Drittstaat es so wollte.

Für die öffentliche Verwaltung in Deutschland ist dieser Vorfall ein Weckruf. Ihre IT stützt sich in Software, Cloud-Diensten, Hardware und Künstlicher Intelligenz weitgehend auf Konzerne außerhalb Europas. Diese Abhängigkeit ist aus drei Gründen hoch bedenklich:

- **Geopolitisch:** Auf internationaler Ebene ersetzt Machtpolitik vielfach Formen der Kooperation. Insbesondere die US-Regierung setzt zurzeit auf Tech-Nationalismus – keine Stärke, sondern eine Gefahr für Deutschland und Europa. Staaten, die über Jahrzehnte enge Partner Europas waren, positionieren sich als erklärte Konkurrenten. Drohungen sind an der Tagesordnung, Vertrauen – das insbesondere rund um das Thema Datenaustausch unerlässlich ist – schwindet rapide. Diese Verwerfungen erfordern eine deutlich höhere Aufmerksamkeit für das Thema digitale Souveränität: Natürlich sollte weiterhin nach Konsens für nationale und internationale Regelungen und neue Technologien gesucht werden, aber wenn die Verfügbarkeit von Cloud-Diensten als Druckmittel in Handelskonflikten genutzt werden sollte, steht die Arbeitsfähigkeit der Verwaltung auf dem Spiel. Ein sogenannter Kill Switch – wie ihn der IStGH-Chefankläger erleben musste – hätte dramatische Folgen.
- **Wirtschaftlich:** Die Preise großer Anbieter steigen kontinuierlich, für SaaS-Lösungen ebenso wie für On-Premises-Lizenzen. Da die Verwaltungen aufgrund erheblicher Lock-in-Effekte nicht frei zwischen verschiedenen Anbietern entscheiden können, fehlt der Wettbewerb. Ergebnis: Die öffentlichen Haushalte werden zunehmend belastet. So gab allein der Bund 2025 rund 480 Millionen Euro für Microsoft-Produkte aus, Tendenz massiv steigend. Ähnlich sieht es auf Länderebene aus, drei Beispiele: In Mecklenburg-Vorpommern sind die Microsoft-Gebühren zwischen 2021 und 2025 von 3,7 Millionen auf 21,1 Millionen Euro gestiegen, in Nordrhein-Westfalen von 29,4 Millionen auf 42,7 Millionen Euro und in Baden-Württemberg von 17,4 Millionen auf 45,6 Millionen Euro. Ein kürzlich erhobenes kommunales Beispiel zeigt eine Steigerung der Lizenzkosten von 7.000 auf 18.000 Euro in vier Jahren.
- **Rechtlich:** Die Verwaltungen müssen die Daten der Bürgerinnen und Bürger – die vielfach in Clouds von US-Konzernen verarbeitet werden – schützen. Der Rechtsschutz ist mit dem EU-US Data Privacy Framework nur scheinbar gegeben. So verpflichtet der CLOUD Act der USA heimische Unternehmen dazu, den US-Behörden bei Bedarf Daten zu übermitteln – auch dann, wenn diese bei einer Tochtergesellschaft in Europa liegen.

Das enorme Innovationstempo und der wachsende Bedarf an leistungsstarker IT, Cloud-Lösungen und KI-Anwendungen – die vornehmlich von US-Konzernen vorangetrieben werden – verschärfen die Situation.

**Die gute Nachricht:** Aus dem steigenden Druck erwächst politische Gestaltungskraft. So sind Ende 2025 Regierungsvertreterinnen und -vertreter aus ganz Europa zum ersten Gipfel für europäische digitale Souveränität in Berlin zusammengekommen.

**Das Ziel:** den Kontinent gemeinsam aus der Dominanz einzelner Anbieter zu lösen. In Deutschland sind erste Schritte bereits getan: Das seit Mai 2026 geltende Vergabebeschleunigungsgesetz verankert digitale Souveränität ausdrücklich als mögliches Zuschlagskriterium. Mit dem Programm CyberGovSecure, der

Rechenzentrumsstrategie, dem Deutschland-Stack und der deutsch-französischen Zusammenarbeit entstehen weitere Bausteine.

Das Momentum ist da. Jetzt kommt es darauf an, Einzelinitiativen in eine kohärente, verbindliche Strategie zu überführen – und die kommunale Ebene von Anfang an mitzudenken.

## 2. Was digitale Souveränität bedeutet – und was nicht

Digitale Souveränität bedeutet, die Kontrolle über die eigenen IT-Systeme und Daten zu behalten: sie selbstbestimmt, sicher und rechtskonform zu betreiben und weiterzuentwickeln. Abhängigkeiten sind dabei bewusst zu steuern, Risiken zu begrenzen und eigene Handlungsoptionen dauerhaft zu sichern.

Was Souveränität nicht ist: ein Abschottungsprogramm oder ein genereller Verzicht auf bewährte Produkte. Im Kern geht es um Entscheidungsfreiheit – also die Fähigkeit, zwischen Technologien und Anbietern zu wählen und im Bedarfsfall auf europäische oder offene Alternativen auszuweichen. Souveränität ist damit kein Zustand, den man einmal erreicht, sondern ein kontinuierlicher Prozess, sich einem Ideal zu nähern. Deshalb braucht es ein iteratives, realistisch umsetzbares Vorgehen, das unterschiedliche Souveränitätsgrade definiert, Fortschritte messbar macht und regelmäßig überprüft.

Dabei müssen Politik und Verwaltung Prioritäten definieren, wo wir unbedingt auf mehr digitale Souveränität abzielen sollten. Aus Sicht von VITAKO stehen dabei insbesondere Fachverfahren mit sensiblen Bürgerdaten wie Melde-, Sozial-, Steuer- oder Gesundheitsdaten im Fokus, außerdem sicherheitskritische Systeme und Bereiche, in denen ein Ausfall oder ein fremder Zugriff die Handlungsfähigkeit des Staates beeinträchtigen und das Vertrauen der Bürgerinnen und Bürger gefährden würde. Hier ist Kontrolle nicht verhandelbar, ein eventuell höherer Aufwand für souveräne Lösungen ist gerechtfertigt. Wo wir hingegen Abstriche machen können? Dort, wo keine sensiblen Daten im Spiel sind und wo sich ein kurzer Systemausfall leicht kompensieren lässt und keine kritischen Folgen hat. In solchen Bereichen ist der pragmatische Einsatz etablierter – auch proprietärer – Produkte vertretbar.

Ein Hinweis zur Standortfrage von Rechenzentren: Es hilft wenig, wenn das Rechenzentrum in Deutschland steht, die genutzte Software aber von einem Mutterkonzern aus einem Drittstaat – der den Strom an Software, Patches und Updates jederzeit unterbrechen kann und nach dem Recht seines Heimatstaates gegebenenfalls zur Datenherausgabe verpflichtet ist – bereitgestellt wird. Souveränität misst sich deshalb nicht am Serverstandort, sondern an der tatsächlichen Kontroll- und Wechselfähigkeit.

## 3. Handlungsfelder – was jetzt zu tun ist

Digitale Souveränität muss als strategische Steuerungsaufgabe verstanden werden – quer durch alle Ebenen: Wir brauchen ein tiefes Verständnis für die Bedeutung des Themas im Bundeskanzleramt und in den Bundesministerien, in Landesministerien und -behörden, in den kommunalen Ratsversammlungen, bei Bürgermeisterinnen und Bürgermeistern bis hin zu den IT-Verantwortlichen. Aus Sicht von VITAKO stehen fünf konkrete Handlungsfelder im Fokus.

### 3.1 Beschaffung strategisch nutzen

Die öffentliche Hand ist der größte IT-Abnehmer des Landes. Diese Marktmacht muss sie gezielt für mehr Souveränität einsetzen. Seit Mai 2026 erlaubt das

Vergabebeschleunigungsgesetz ausdrücklich, digitale Souveränität als Zuschlagskriterium und Ausführungsbedingung zu berücksichtigen. Diese Möglichkeit muss nun konsequent und verbindlich genutzt werden.

Zugleich muss der Staat seine Rolle als Ankerkunde aktiv wahrnehmen und gebündelte IT-Aufträge für den Aufbau heimischer und europäischer Anbieter einsetzen. Verhandlungen mit großen Anbietern aus Drittstaaten sind möglichst zentral zu führen, um Handlungsmacht und Synergien zu schaffen. Bund und Länder müssen sich zu diesen Ansätzen klar bekennen und gemeinsam mit den Kommunen Verhandlungsmacht aufbauen.

### 3.2 Offene Alternativen ausbauen und verlässlich finanzieren

Open-Source-Software ist ein Schlüssel, um Lock-in-Effekte – also die Abhängigkeit von einzelnen Anbietern – zu vermeiden. Das Prinzip ist simpel: Programmiercode wird von den Urheberinnen und Urhebern öffentlich auf Plattformen im Internet zur Verfügung gestellt. Die Nutzenden zahlen in der Regel eine Gebühr für den Support und können mit frei gewählten Partnern eigene Softwarelösungen erstellen.

An vielen Stellen im IT-Betrieb der öffentlichen Verwaltung, etwa beim Betrieb von Servern und Datenbanken, ist Open-Source-Software bereits verbreitet. An den IT-Arbeitsplätzen hingegen – also bei Office-Programmen oder in der Kommunikation – dominieren proprietäre Produkte. Gerade hier muss die Entwicklung von Open-Source-Alternativen wie openDesk weiter vorangetrieben werden. Für eine möglichst hohe Nutzerakzeptanz gilt es, die Bedienbarkeit stetig weiter zu verbessern und neue Funktionen hinzuzufügen, wie dies auch bei den gängigen proprietären Produkten geschieht. Ziel ist dabei nicht, proprietäre Lösungen vollständig zu ersetzen, sondern eine hinreichend große Nutzerbasis aufzubauen.

Ein positives Beispiel in Sachen Open Source ist das Land Schleswig-Holstein. Im Rahmen seiner Open-Source-Strategie hat das Bundesland seit Oktober 2025 bereits mehr als 40.000 E-Mail-Postfächer von Microsoft Exchange und Outlook auf die Open-Source-basierten Programme Open-Xchange und Thunderbird umgestellt. Weitere Programme sollen folgen.

Der Staat ist gefordert, Open-Source-Lösungen zu fördern und in Ausschreibungen bevorzugt zu behandeln. Zudem muss der Bund das Zentrum für Digitale Souveränität (ZenDiS) dauerhaft finanzieren und so aufstellen, dass es Kommunen konkret dabei unterstützen kann, leistungsfähige Open-Source-Software koordiniert einzusetzen.

### 3.3 Souveräne Infrastruktur bereitstellen

Mit dem Deutschland-Stack hat der IT-Planungsrat im März 2026 erstmals einen verbindlichen Plattformkern für Bund, Länder und Kommunen beschlossen. Das ist der richtige Weg, solange wesentliche Anforderungen der digitalen Souveränität auch eingehalten werden: Der D- Stack muss auf offenen Schnittstellen basieren und darf nicht unter neuem Etikett alte Abhängigkeiten fortschreiben. Wichtig auch: Die Deutsche Verwaltungscloud – die inzwischen rund 70 Cloud-Services erfolgreich anbietet und massiv wächst – muss ein wesentlicher Teil des Deutschland-Stacks werden und genügend Angebote (SaaS, PaaS, IaaS) von öffentlichen IT-Dienstleistern und europäischen Anbietern bereithalten. Nur so sinkt die Abhängigkeit tatsächlich.

### 3.4 Interoperabilität und Wechselfähigkeit verbindlich machen

Ein wesentlicher Faktor, um öffentlichen Verwaltungen und deren IT-Dienstleistern einen einfachen Wechsel zwischen verschiedenen Software-Produkten, SaaS-Lösungen und Cloud-Infrastrukturen zu ermöglichen, ist die möglichst reibungslose Übertragung der Datenbestände von einem System zum anderen. Bisher sind solche Umstellungen mit hohem Arbeitsaufwand und Kosten verbunden, wodurch wiederum Lock-in-Effekte entstehen. Um diese zu vermeiden, müssen für die öffentliche Verwaltung grundlegende Datenstandards geschaffen und zusammen mit offenen Schnittstellen für alle dort eingesetzten Produkte eingefordert werden. Der EU Data Act – seit September 2025 anwendbar – stärkt hier die Rechte der Verwaltungen.

Deshalb gilt: Für alle relevanten Produkte sind offene Standards und Schnittstellen verbindlich einzufordern und als K.-o.-Kriterium in jeder Ausschreibung umzusetzen. Zudem ist der EU Data Act konsequent durchzusetzen, damit Verwaltungen zwischen verschiedenen Anbietern von Produkten und Dienstleistungen auch tatsächlich wechseln können.

### 3.5 Souveränität und Sicherheit zusammendenken

Souveränität und Sicherheit gehören zusammen: Ein System, das man nicht schützen kann, kontrolliert man nicht wirklich. Mit CyberGovSecure hat der Bund einen koordinierten Rahmen für die Cybersicherheit geschaffen – bislang jedoch nur für die Bundesverwaltung. Die kommunale Ebene, die täglich Ziel von Angriffen ist, bleibt außen vor. Ein weiteres wichtiges Projekt ist der geplante Cyberdome des Bundesinnenministeriums, der als Frühwarn- und Schutzsystem Cyberangriffe auf staatliche Institutionen und Kritische Infrastrukturen in Echtzeit erkennen und Schäden minimieren soll. Die Kommunen müssen bei den Planungen eng eingebunden werden und später von dem System umfassend profitieren.

### 3.6 Einheitliche Definitionen schaffen

Damit Bund, Länder, Kommunen und öffentliche IT-Dienstleister auf einer einheitlichen Grundlage handeln können, muss die digitale Souveränität auf Basis nachvollziehbarer Kriterien bundesweit definiert werden. Ein solches Modell muss unterschiedliche Schutzbedarfe und Souveränitätsgrade berücksichtigen und handhabbar sein – zusätzliche bürokratische Hürden sind strikt zu verhindern.

### 3.7. Nach Schutzbedarf und Machbarkeit priorisieren

Angesichts begrenzter Ressourcen kann digitale Souveränität nicht gleichzeitig mit identischer Intensität für sämtliche IT-Systeme und Verwaltungsverfahren verfolgt werden. Notwendig ist eine risikobasierte Priorisierung, bei der insbesondere Fachverfahren mit sensiblen Bürgerdaten, kritische Verwaltungsprozesse und unverzichtbare Leistungen der kommunalen Daseinsvorsorge im Mittelpunkt stehen. Im Fokus stehen deshalb insbesondere Bereiche wie Sozialleistungen, Meldewesen, Gesundheit oder kommunales Finanzwesen. Gleichzeitig sind technische Machbarkeit, Abhängigkeiten und wirtschaftliche Tragfähigkeit zu berücksichtigen.

### 3.8. Finanzierung sichern

Digitale Souveränität ist nicht für umsonst zu haben. Die entsprechenden Maßnahmen verursachen insbesondere in der Transformationsphase erheblichen Zusatzaufwand. So müssen die kommunalen IT-Dienstleister bestehende Technologien evaluieren, neue

Kompetenzen aufbauen und gegebenenfalls alternative Plattformen, Infrastrukturen und Betriebsmodelle parallel zu bestehenden Lösungen entwickeln und betreiben.

Die damit einhergehenden Kosten lassen sich nicht ohne Weiteres über bestehende Produktpreise und Entgeltmodelle refinanzieren, zumal kommunale Auftraggeber selbst unter erheblichem finanziellem Druck stehen. Bund und Länder müssen deshalb geeignete Finanzierungsmechanismen schaffen.

## 4. Masterstrategie erarbeiten – noch in dieser Legislatur

Digitale Souveränität ist eine gesamtstaatliche Aufgabe, deren Umsetzung derzeit auf zahlreiche Akteure, Initiativen und föderale Ebenen verteilt ist. Folge: Verantwortlichkeiten und operative Zuständigkeiten sind nicht immer ausreichend erkennbar. Umso wichtiger ist es, dass der Bund – beispielsweise unter Leitung des Bundesministeriums für Digitales und Staatsmodernisierung (BMDS) – eine Masterstrategie digitale Souveränität erarbeitet. Diese Masterstrategie definiert Ziele, Standards und Prioritäten, legt Verantwortlichkeiten fest und beschreibt einen verbindlichen Fahrplan bis zum Ende der Legislatur. Dabei gilt es, die zahlreichen Initiativen wie Gaia-X, das ZenDiS mit seinen Projekten openDesk und openCode, die Deutsche Verwaltungscloud, den Sovereign Cloud Stack oder diverse Ausschreibungen für Cloud-Broker – die allesamt auf das Ziel der digitalen Souveränität einzahlen – einzubinden. Auch der Bereich Hardware samt Chip-Entwicklung und -produktion ist zu berücksichtigen.

Wichtig dabei: Eine Strategie ist nur so viel wert, wie sich ihr Fortschritt nachweisen lässt. Es gilt, anhand klarer Indikatoren festzustellen, ob bestimmte Maßnahmen wirken, und gegebenenfalls nachzusteuern. Mögliche Kennzahlen lauten:

- Anteil von Open-Source-Software
- Anteil von Ausschreibungen, die Souveränität als Kriterium berücksichtigen
- Marktanteil europäischer Cloud-Anbieter im öffentlichen Sektor
- Durchschnittliche Dauer und Kosten eines Anbieterwechsels
- Lizenzausgaben für ausländische Anbieter
- Supportausgaben für OSS

Kennzahlen dieser Art gehören in die Gesamtstrategie des Bundes, verbunden mit regelmäßigen Berichtspflichten. Erst dann wird aus dem Anspruch, digitale Souveränität zu verfolgen, ein steuerbares Ziel.

## Rolle der kommunalen IT-Dienstleister

Kommunale IT-Dienstleister betreiben einen wesentlichen Teil der digitalen Infrastruktur der öffentlichen Verwaltung. Ihre Rolle ist es einerseits, den Verwaltungen digital souveräne Lösungen zu ermöglichen. Anders als gewinnorientierte Unternehmen haben sie als Träger der öffentlichen Hand ein intrinsisches Interesse am Funktionieren der Verwaltung. Sie treiben Standardisierung und Weiterentwicklung voran, bündeln Bedarfe, beraten bei Technologieentscheidungen, stellen selbst souveräne Infrastrukturen bereit – und stehen den Kommunen als stabile Partner zur Seite. Besonders wichtig dabei: Seit Jahren forcieren sie breit angelegte Kooperationen, ohne die eine Aufgabe in dieser Größenordnung nicht zu bewältigen wäre. Andererseits sind sie bei der Wahl von IT-Produkten vielfach abhängig von US-Anbietern. Vor diesem Hintergrund wirbt VITAKO gegenüber der Politik nachdrücklich dafür, die Rahmenbedingungen auch für seine Mitglieder zu verbessern.

## Die föderale Dimension

Digitale Souveränität gelingt nur gesamtstaatlich. Der Bund gibt den Rahmen vor, doch entschieden wird an vielen Stellen.

- Länder: Sie verantworten einen Großteil des Verwaltungsvollzugs. In ihrem Bereich entscheiden sie über Beschaffung und Fachverfahren und können offene Lösungen erproben. Schleswig-Holstein zeigt seit Jahren, dass eine konsequente Open-Source-Strategie trägt.
- IT-Planungsrat: Er ist das politische Steuerungsgremium von Bund und Ländern; die Kommunen sind über ihre Spitzenverbände beteiligt. Hier werden verbindliche Standards und Rahmen gesetzt, beispielsweise zum Deutschland-Stack. Der Bund hat damit die Chance, Souveränität föderal verbindlich zu verankern, statt sie dem Zufall der einzelnen Häuser zu überlassen.
- FITKO: Sie ist die Umsetzungsstelle des IT-Planungsrats, bringt dessen Beschlüsse operativ in die Fläche, koordiniert gemeinsame Vorhaben und stellt Fördermittel bereit. Hier entscheidet sich vielfach, ob aus Beschlüssen gelebte Praxis wird.

Und die Kommunen? Sie wollen vor allem eines: funktionierende, bezahlbare Lösungen im Alltag. Digitale Souveränität ist für sie selten Chefsache und in Zeiten gravierender Haushaltslöcher selten prioritär. Umso wichtiger ist es, sie gezielt zu unterstützen und mit einer bundesweit greifenden Masterstrategie einen klaren Rahmen zu bieten.

## Office-Anwendungen: Kommunen beim Kurswechsel mitnehmen

Cloudbasierte Office-Anwendungen großer internationaler Softwareanbieter gehören in den allermeisten Verwaltungen zum Arbeitsalltag. Umso wichtiger ist es, dass der angekündigte Kurswechsel des Bundes geordnet verläuft. Digitalminister Wildberger will die Abhängigkeit der Verwaltung von einzelnen großen Anbietern schrittweise verringern. Dieser Weg ist richtig. Der Bund muss dafür einen klaren, belastbaren Zeitplan samt tragfähiger Interimslösungen vorlegen – und dabei die Länder und Kommunen sowie deren IT-Dienstleister von Anfang an einbinden.