Stellungnahme zur Weiterentwicklung des ZenDiS Katalogs für digitale Souveränität:

Empfehlungen für eine messbare, umsetzbare Bewertung

1 Einleitung

Die Zentrale Digitale Souveränität (ZenDiS) hat mit ihrem Konsultationsprozess einen wichtigen Meilenstein gesetzt: die Festlegung von Kriterien zur Bewertung digitaler Souveränität in der öffentlichen Verwaltung. Für uns als etabliertes Open-Source-Beratungsunternehmen bietet dieser Ansatz die Gelegenheit, die Stärken, wie Transparenz, Wechselmöglichkeiten und gestalterische Freiheit, systematisch in einen evaluierbaren Rahmen zu überführen und gleichzeitig die spezifischen Belange der Verwaltung zu adressieren. In unserer Stellungnahme wollen wir zeigen, welche Aspekte aus unserer Praxis besonders gewichtet werden sollten, wie Messbarkeit und Operationalisierung gelingen können und welche Nachweisformen sowohl valide als auch im Behördenalltag praktikabel sind.

Der aktuelle politische Rahmen unterstreicht die Dringlichkeit dieses Vorhabens. Der Koalitionsvertrag[1] der Bundesregierung betont den Ausbau offener Standards und die Stärkung der digitalen Souveränität als zentrales Ziel der Digital-Agenda 2025-2030[2]. Auf EU-Ebene wird mit dem „Digital Sovereignty Package“[3] und der neuen Open-Source-Strategie[4] der Kommission die Notwendigkeit hervorgehoben, Abhängigkeiten von einzelnen Anbietern zu reduzieren und die Kontrolle über kritische Infrastrukturen zurückzugewinnen. Gleichzeitig fordert der Nationale Rat für digitale Verwaltung, dass Bewertungsinstrumente transparent, nachvollziehbar und unmittelbar in Haushalts- und Planungsprozesse integrierbar sein müssen, um Investitionen in zukunftsfähige, offene Lösungen zu rechtfertigen. In diesem Umfeld liefert der ZenDiS-Katalog die fachliche Grundlage, während unsere Expertise die praktische Umsetzbarkeit und die politischen Vorgaben in konkrete, messbare Praxis übersetzt.

Unserer Stellungnahme zu dem derzeit vorliegenden Katalog konzentriert sich auf Lücken, denen wir in der Praxis vermehrt begegnen.

2 publicplan Kernbotschaften

- Der ZenDiS-Katalog muss den Übergang vom IST-Zustand zum definierten SOLL-Zustand (gewünschter souveräner Betrieb) explizit berücksichtigen, damit die Verwaltung souverän handeln kann und die eingesetzten Lösungen keine fremdbestimmten Abhängigkeiten aufweisen.

- Neben der Erfassung der Kriterien muss festgelegt werden, wie, wann und wie häufig gemessen und bewertet wird. Damit werden die Ergebnisse steuerbar, wiederholbar und unmittelbar in Haushalts- sowie Planungsprozesse integrierbar.

[1] Koalitionsvertrag 2025 | Bundesregierung
[2] Digitale Agenda | BMWE
[3] Commission opens call for evidence on Open-Source Digital Ecosystems | Shaping Europe’s digital future
[4] Open source software strategy - European Commission

3 Kriterien digitale Souveränität

Digitale Souveränität lässt sich in zwei wesentliche Aspekte gliedern. Auf der einen Seite sollten souveräne IT-Lösungen wenige Abhängigkeiten enthalten, indem diese offene Standrads nutzen, einen breiten Markteinsatz haben und keine Einflussnahme oder Zugriff durch externe Organisationen erlauben. Auf der anderen Seite muss die Organisation selbst souverän sein, indem sie Veränderungen gezielt und eigenständig durchführen kann, ohne von externen Akteuren abhängig zu sein.

Da wir auf der vorhandenen Lösungslandschaft aufbauen, die im Rahmen der Digitalisierungen bereits im großen Umfang entstanden ist, sollte sich der Prozess der Veränderung dieser Lösungslandschaft in den Kriterien widerspiegeln. Daher haben wir den Kriterienkatalog entsprechend ergänzt.

Die Umsetzbarkeit der Kriterien wird durch eine transparente und nachvollziehbare Bewertung der Kriterien ermöglicht. Wir empfehlen daher die Kriterien, analog zu Ausschreibungen, in A- und B-Kriterien zu unterscheiden. A-Kriterien sind erfüllt oder nicht erfüllt und B-Kriterien werden nach ihrem Grad der Erfüllung bewertet. Außerdem sollte eine Methodik an die Hand gegeben werden, wie Kriterien bewertet werden und in welchen Intervallen dies wiederholt werden soll.

Wir schlagen folgendes Vorgehen zur Bewertung vor: wir empfehlen die Anwendung etablierter Standards wie des CMMI Reifegradmodell zur Bewertung der Kriterien, um die Fähigkeit der Organisation zu beurteilen. Im Bereich IT-Sicherheit sollte der IT-Grundschutz des BSI[5] die Grundlage für die Bewertung bilden. Entsprechend des Schutzbedarfs ist auch die Bewertung der Souveränität vorzunehmen.

Neben den Kriterien sollte vor allem ein Regelprozess zur Erfassung und Bewertung der Aspekte etabliert werden. Die Prozesse sind das Gedächtnis der Organisation und gewährleisten eine kontinuierliche Beschäftigung und Entwicklung des Themas. Daher sollte mindestens alle drei Jahre eine umfassende Bewertung vorgenommen werden und anschließend darauf basierend die Maßnahmen abgeleitet werden. Die Umsetzung der Maßnahmen sollte jährlich durch ein übergeordnetes Gremium, wie dem Landes-CIO und der Behördenleitung geprüft werden. Damit wird auch die Einbindung in die übergeordnete Strategie sichergestellt, da untergeordnete Behörden teilweise keinen Einfluss auf die Inhalte der Strategie haben, sondern rein für die operative Umsetzung zuständig sind.

4 Fazit

Durch die vorgeschlagenen Ergänzungen erhält der ZenDiS-Katalog sowohl eine klare strukturelle Gliederung als auch einen praktikablen Umsetzungsrahmen, der die politische Vorgabe nach digitaler Souveränität mit den konkreten Bedürfnissen der öffentlichen Verwaltung verknüpft. Damit liegt ein Instrument vor, das nicht nur theoretische Vorgaben macht, sondern konkrete Handlungsleitfäden für einen schrittweise, nachvollziehbare und in die Haushalte- sowie Planungsprozesse integrierbare Transformation bietet.

[5] BSI IT-Grundschutz

Gleichzeitig sollte bewusstwerden, dass wahre digitale Souveränität erst entsteht, wenn die gesamte Gesellschaft daran teilhaben und den Nutzen dieser Systeme erleben kann. Sie muss auf einem einheitlichen, allgemeinen anerkannten Standard beruhen – vergleichbar mit der DIN-Norm im Baugewerbe – um Vergleichbarkeit, Transparenz und langfristige Verlässlichkeit über Behördengrenzen hinweg zu gewährleisten. Nur so lässt sich eine nachhaltige, gemeinwohlorientierte digitale Infrastruktur realisieren, die sowohl administrative Effizienz als gesellschaftlichen Mehrwert schafft.

Ansprechpartner:in / Autor:in

Heiko Zeippert
IT-Architekt und Deutschland-Stack Experte
✉ Heiko.Zeippert@publicplan.de

Christina Hasse
Senior Beraterin
✉ Christina.Hasse@publicplan.de

publicplan.

Berlin ▪ Düsseldorf ▪ München

publicplan GmbH
Kennedydamm 24
40476 Düsseldorf

Tel.: +49 (0) 211 635501-80
Fax: +49 (0) 211 635501-89
info@publicplan.de

publicplan.de

Geschäftsführer: Dr. Christian Knebel
Amtsgericht Düsseldorf, HRB 63966
USt-Id-Nr. DE273003539

Anhang: Kriterienkatalog digitale Souveränität

A	Organisation und Fähigkeiten		Ziel	Kriterium	Bewertung
A1	Strategie	Ist Digitale Souveränität in der Digitalstrategie und den übergeordneten Leitlinien der Organisation verankert?	● ◆	A	-
A2	IT-Governance & Management	Sind Verantwortlichkeiten, Prozesse und Steuerungsstrukturen im IT-Betrieb definiert und umgesetzt?	● ◆	B	ITIL als Standard, Umsetzung nach CMMI Reifegradmodell[6] messen.
A3	Risikomanagement	Werden technologische, organisatorische und strategische Risiken im Hinblick auf Abhängigkeiten erfasst und gesteuert?	● ◆ ■	B	CMMI Reifegradmodell
A4	Beschaffung und Vergabe	Werden Beschaffungsprozesse so gestaltet, dass Wettbewerb, Offenheit und Alternativen berücksichtigt werden?	● ◆ ■	A	-
A5	Auftraggeberfähigkeit	Ist die Organisation in der Lage, IT-Projekte eigenständig zu steuern und Anbieter wirksam zu kontrollieren?	● ◆	A	-
A6	Kompetenzen	Verfügt die Organisation über die nötigen (IT-)Kenntnisse, Fachkräfte und Wissensbestände, um souverän handeln zu können?	● ◆ ■	A	-
A7	Transformation & Changemanagement	Fähigkeit die Organisation durch die Veränderung beim Erreichen der digitalen Souveränität zu bringen und alle Mitarbeiter dabei mitzunehmen	●	B	CMMI Reifegradmodell
A8	Planung & Ressourcen	Fähigkeit langfristig Abhängigkeiten durch eine gezielte Planung aufzulösen und Schritt für Schritt die strategischen Ziele zu erreichen	● ■	A	-

[6] https://cmmiinstitute.com/ (Abgerufen am 23.04.2026)

B	Digitale Anwendungen und Dienste		Ziel	Kriterium	Bewertung
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?		B	Abdeckungsgrad in Prozent
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?		A	-
B3	Anwendungsarchitektur / Modularität	Sind Anwendungen portabel und modular aufgebaut und technisch entkoppelbar?		A	-
B4	Standards	Nutzen Anwendungen offene Schnittstellen und etablierte Standards, um Austauschbarkeit und Integration zu ermöglichen?		A	-
B5	Abhängigkeit auf Software-Ebene	In welchem Umfang bestehen Lock-in-Risiken durch proprietäre Software oder fehlende Alternativen? Hier sind nicht nur Lock-in-Risiken zu bewerten, sondern die Feststellung, wo bereits ein Lock-In besteht und welche Auswirkungen dieser hat.		A	-

C	Daten		Ziel	Kriterium	Bewertung
C1	Datenlokation	Wo werden Daten gespeichert und verarbeitet (lokal, EU, Drittstaaten) und wie ist dies zu kontrollieren?		B	Katalog mit Anwendungen und Speicherort
C2	Datensicherheit	Werden Daten umfassend verschlüsselt und gibt es entsprechende Konzepte sowie technische und organisatorische Maßnahmen, welche die Datensicherheit Ende-zu-Ende gewährleisten?		A	-
C3	Datenschutz	Werden rechtliche Vorgaben (z. B. DSGVO) eingehalten und durch technische sowie organisatorische Maßnahmen abgesichert?		A	-

C4	Datenstrukturen	Sind Daten in offenen, interoperablen Formaten abgelegt, sodass Portabilität und Wiederverwendbarkeit gesichert sind? Es ist klar definiert in welchen Datenfeldern bzw. Datenstrukturen die jeweiligen fachlichen Informationen abgespeichert werden.		B	Katalog mit den Daten und Bewertung der Formate
C5	Datenquellen	Werden in der Anwendung zusätzliche Datenquellen genutzt und wie werden diese Daten ins System eingebracht und wozu sind diese Notwendig, z.B. Wiederverwendung von Stammdaten.		A	-

D	Betrieb und Infrastruktur		Ziel	Kriterium	Bewertung
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?		B	Bewertung der Bindung (Austauschbar, Aufwändig Austauschbar, nicht Austauschbar)
D2	Kundenverhältnis	Erlaubt das Kundenverhältnis eine Einflussnahme auf Software-Entwicklung und digitale Dienste, beispielsweise durch eine transparente Release-Planung und aktivem Anforderungsmanagement?		A	-
D3	Exit-Fähigkeit	Ist ein Anbieterwechsel oder Rückführung in Eigenbetrieb realistisch und erprobt?		A	-
D4	Resilienz & Business Continuity	Wie robust sind die Systeme gegenüber Ausfällen, Krisen oder Angriffen und wie schnell ist ein Wiederanlauf möglich?		B	Bewertung der Robustheit in Bezug auf die Notwendigkeit auf Basis des Schutzbedarfes
D5	Sicherheit und Compliance im Betrieb	Werden regulatorische und organisatorische (EU-)Anforderungen im laufenden Betrieb durchgängig überprüft und eingehalten?		A	-
D6	Wartungsvereinbarungen	Gibt es einen Wartungsvertrag, welcher sicherstellt, dass die Software bei Schwachstellen innerhalb einer angemessenen Zeit beseitigt werden? Wie wird die dauerhafte Wartung der Software inkl. Verwendeter Bibliotheken sichergestellt?		A	-