Mai 2026

Öffentliche Konsultation - Diskussionspapier

Kriterien für Digitale Souveränität – aus messbar wird machbar

Stellungnahme von Frank Ingernrieth

Rechtsanwalt Frank Ingenrieth, LL.M.

0 Über den Autor

Frank Ingenrieth, LL.M. (**Gutachter**) ist Führungskraft und niedergelassener Anwalt mit über 15 Jahren interdisziplinärer, internationaler Erfahrung im Bereich Steuerung von Datenschutz- und Regulierungsstrategien für nachhaltige, innovationsorientierte Lösungen. Sein Schwerpunkt liegt im Medien-, Internet- und Datenschutzrecht, sowie verbundenen Rechtsgebieten, z.B. Mietrecht, oder wechselwirkende Rechtsgebiete, etwa dem Wettbewerbs- und Kartellrecht, sowie im Bereich der Fragen der Good Governance.[1]

Seine Erfahrung sammelte Frank Ingenrieth während seines beruflichen Werdegangs, inklusive seiner Ausbildung, in internationalen Großkanzleien, datenschutzrechtlicher Aufsichtsbehörden, internationaler Konzerne, gemeinnütziger Organisationen. Er veröffentlicht regelmäßig, entweder im Rahmen von juristischer Fachliteratur, Fachkommentare, sowie in Form von Diskussionsrunden und Panels[2].

Diese Stellungnahme wurde unabhängig und ohne Auftrag durch etwaige Mandant*Innen erstellt. Die Stellungnahme und die Anmerkungen basieren auf der langjährigen praktischen Erfahrung des Autors in der Entwicklung und Durchsetzung von Konformitätsbewertungsprogrammen, inklusive solcher Prüfprogramme, die aufgrund ihrer rechtlichen Vermutungswirkungen behördlicher Anerkennung bedürfen.

Pflicht- und Kontaktinformationen des Autors

Richard-Sorge-Straße 69a
10249 BERLIN

Fon +49 30 985 387 95
Fax +49 30 521 036 88
E-Mail office@ingenrieth-online.de

Steuer-Nummer 14/358/01684,
FA Friedrichshain-Kreuzberg.

Ich optiere gem. **§ 19 UstG** als Kleinunternehmer.

IBAN DE22 5002 4024 7497 0388 01

Zuständige Kammer
Rechtsanwaltskammer Berlin, Littenstraße 9, 10179 Berlin

In Deutschland verliehene **Berufsbezeichnung**
Rechtsanwalt

wesentliche **berufsrechtliche Regelungen**

- Bundesrechtsanwaltsordnung
- Berufsordnung
- Rechtsanwaltsvergütungsgesetz.

Diese und weitere können auf der Webseite der Rechtsanwaltskammer Berlin abgerufen werden.

1 Näheres über den Autor kann auf der Webseite der Kanzlei abgerufen werden: https://ingenrieth-online.de/de/ueber.

2 Eine Übersicht der Veröffentlichungen kann auf der Webseite der Kanzlei abgerufen werden: https://ingenrieth-online.de/de/publikationen.

Inhaltsverzeichnis

1 Executive Summary

- Gegenstand der Betrachtung ist das Diskussionspapier in der Fassung „März 2026“.
- Die Empfehlungen betreffen sowohl generell-strukturelle Aspekte (Abschnitt 3), als auch konkrete Aspekte zu den einzelnen Dimensionen (Abschnitt 4).
- Auf Basis der theoretischen Konzepte und Ziele von Kriterienkatalogen (Abschnitt 3.1.1) wird empfohlen den Kriterienkatalog als Reifegradmodell auszubauen (Abschnitt 3.1.2).
- Konkret wird empfohlen ein „offenes Reifegradmodell“ zu entwickeln (Abschnitt 3.1.2). konkret wird von einer geschlossenen Ausgestaltung im Reifegradmodell für Digitale Souveränität abgeraten, obgleich sich in vielen Bereichen eine Dreistufigkeit (low/basic, essential, high) etabliert.
- Es wird empfohlen, die Zielsetzung des Kriterienkatalogs zu klären und die Dimensionen und Kriterien streng anhand dieser Zielsetzung auszugestalten (Abschnitt 3.2).
- Für eine objektive und vergleichbare Erfassung der Umstände müssten die Dimensionen und die Objectives in konkrete Kriterien überführt werden. Aufgrund der hohen Dynamik sollte hierbei insbesondere auch auf ergänzende Erläuterungen zurückgegriffen werden, inklusive Beispielen und Empfehlungen (Abschnitt 3.3).
- Es sollte deutlich(er) herausgearbeitet werden, wie durch den Kriterienkatalog die Aspekte der Digitalen Souveränität ergänzt werden (Abschnitt 3.4).
- Es sollte auf unnötige Redundanzen verzichtet werden, da diese letztlich zu einer vermeidbaren Hürde bei der Implementierung führen. Redundanzen lösen – auch ungewollt – Auslegungskonflikte aus, insbesondere soweit die Redundanz nicht wort- und kontextidentisch ist (Abschnitt 3.4).
- Wenn und soweit Elemente des EU CSG oder der BSI C3A für förderlich aus Sicht des Diskussionspapiers erachtet werden, und eine Übernahme der Inhalte zielführend und nicht vermeidbar ist, sollte allenfalls ein (statischer) Verweis auf die jeweiligen Kriterien erfolgen und diese somit inkorporiert werden (Abschnitt 3.4).
- Soweit Informationen bereits aufgrund anderer Kriterienkataloge objektiv und sachdienlich erfasst werden, etwa Lieferketten (Vendor Management), oder anwendbare Jurisdiktionen inklusive der implementierten Mitigationsmaßnahmen, so sollten die Kriterien des Diskussionspapiers die Öffentliche Verwaltung dahingehend ertüchtigen und messen, ob diese bereits bestehenden Kriterienkataloge bekannt und verwendet werden. Dies kann auch eine kritische Auseinandersetzung mit den jeweiligen Schwächen der existierenden Kriterienkataloge sein, mit der Folge, dass die Öffentliche Verwaltung diese Schwächen durch eigene, ergänzende Maßnahmen neutralisiert (Abschnitt 3.4).

- Die Risikobetrachtung sollte eine eigene Dimension darstellen (Abschnitt 3.5).
- Die Möglichkeit individueller Maßnahmen sollte aufrecht erhalten werden (Abschnitt 3.5).
- Es wird empfohlen, die Dimension A stärker auf die nicht-technischen Aspekte einer organisatorischen Ertüchtigung zu fokussieren, und dabei die Erkenntnisse der weiteren Dimensionen nutzbar zu machen (Abschnitt 4.1).
- Es wird empfohlen, etwaige technische Aspekte entweder auf Basis der bereits entwickelten weiteren Kriterienkataloge zu inkludieren, oder in eigene, noch zu entwickelnde Kriterienkataloge auszulagern und hierdurch die Zielsetzung des Diskussionspapiers zu schärfen, und somit schnellere, und nachhaltigere Effekte zu erzielen (Abschnitt 4.1).
- Generell wird für die weiteren Dimensionen (B bis D) empfohlen, Redundanzen zu reduzieren, die Zielsetzung der Dimensionen zu schärfen, und im Ergebnis zunächst den Fokus auf eine referenzielle Inklusion in Dimension A zu legen (Abschnitte 4.2, 4.3, 4.4).

2 Gegenstand der Stellungnahme und Struktur

Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (**ZenDiS**) hat ein Diskussionspapier zur Digitalen Souveränität der öffentlichen Verwaltung publiziert.

Das ZenDiS bittet um Stellungnahme. Das Diskussionspapier mit dem Titel „Kriterien für Digitale Souveränität – aus messbar wird machbar“[3] zielt darauf ab, Kriterien zu entwickeln, die den Grad der Digitalen Souveränität in der Öffentlichen Verwaltung messbar machen.

Dem Diskussionspapier liegt die These zu Grunde, dass sich aus der „Messbarkeit“ eine „Machbarkeit“ ergäbe oder jedenfalls erleichtere.[4]

Der Kriterienkatalog wurde nach eigener Angabe des ZenDiS während des Konsultationsphase weiterentwickelt.[5] Es ist aber nicht erkennbar, inwieweit dieser Workshop unmittelbare Änderungen im Diskussionspapier zur Folge hatte. Insoweit bezieht sich diese Stellungnahme weiterhin auf das Diskussionspapier, Stand März 2026.

Während der dynamische und kollaborative Ansatz des ZenDiS positiv hervorzuheben ist, wäre eine inhaltliche Änderung während einer Konsultationsphase auch nicht zielführend, da sich die Stellungnahmen auf ein sich stets veränderndes Objekt bezögen und im Ergebnis keine Vergleichbarkeit ermöglichten. Die Konsultationsphase erscheint hinreichend lang für eine zielgerichtete Kommentierung und zugleich kurz genug, um eine dynamische und zeitnahe Weiterentwicklung durch das ZenDiS zu ermöglichen.

Die Struktur der Stellungnahme gliedert sich in Allgemeine Anmerkungen (siehe Abschnitt 3) und Spezifische Anmerkungen (siehe Abschnitt 4).

3 Abrufbar unter: https://www.zendis.de/media/pages/newsroom/publikationen/konsultationsprozesskriterien/97c259289f-1774439296/zendis_diskussionspapier-kriterien-bewertung-digitaler-souveraenitaet.pdf

4 Siehe Kapitel 2 des Diskussionspapiers.

5 Siehe Hinweis auf einen Workshop vom 29. April 2026 auf https://souveränitätscheck.de mit Verweis auf die Ergebnisse unter https://www.zendis.de/media/pages/newsroom/publikationen/konsultationsprozesskriterien/97c259289f-1774439296/zendis_diskussionspapier-kriterien-bewertung-digitaler-souveraenitaet.pdf

3 Allgemeine Anmerkungen

Allgemeine Anmerkungen beziehen sich auf strukturelle Überlegungen und adressieren somit sowohl den generellen Ansatz des Diskussionspapiers sowie dessen Prämissen.

Eine erste abstrakte Einordnung des Diskussionspapiers durch den Autor erfolgte bereits zum 7. April 2026[6]. Diese Stellungnahme wird auf die dort genannten, ersten Eindrücke näher eingehen.

Die Allgemeinen Anmerkungen beziehen sich unter anderem auf

- **konzeptionelle Überlegungen** über die Potentiale von Kriterienkatalogen (siehe 3.1)
- Klarheit bezüglich des **Gegenstands der Betrachtung** (siehe Abschnitt 3.2)
- Existenz von und erforderliche **Klarheit bezüglich der Kriterien** (siehe Abschnitt 3.3)
- **Synergiepotentiale** hinsichtlich anderer Souveränitätskriterien (siehe Abschnitt 3.4)
- **Risikobetrachtung** (siehe Abschnitt 3.5)

6 Siehe *Ingenrieth*, ZenDiS calls for feedback on Digital Sovereignty Criteria - Reference and First Comment, https://ingenrieth-online.de/de/aktuelles/detail/zendis-calls-for-feedback-on-digital-sovereignty-criteria-reference-and-first-comment

3.1 konzeptionelle Überlegungen über die Potentiale von Kriterienkatalogen

Zunächst ist zu klären, welches **Ziel der Kriterienkatalog verfolgt**. Hierzu sollten zunächst die theoretischen Überlegungen der möglichen Konzepte bedacht werden und sodann auf die ersichtliche Intention des Diskussionspapiers übertragen werden.

3.1.1 theoretische Optionen und Konzepte

Kriterienkataloge können unterschiedliche Zielrichtungen entfalten.[7] Übergeordnetes Ziel ist stets, die Konformität mit den Kriterien in einer vergleichbaren Form überprüfbar zu machen. Hierbei kann das weitere Ziel sein, dass

- eine **Eigenschaft zu einem bestimmten Zeitpunkt** bestätigt wird – etwa Produkt(-sicherheits-)zertifizierungen – und/oder sich aus diesem Umstand bestimmte Wahrscheinlichkeiten einer Konformität für die Zukunft ableiten lassen – etwa in der Regel durch zertifizierte Managementsysteme –
- eine **Aussage über eine Eigenschaft retrospektiv in einem bestimmten Zeitraum** getroffen wird – in der Regel durch Audit-Programme, etwa SOC oder BSI C5.

Während eine Zertifizierung grundsätzlich binär pro Kriterium erfolgt (erfüllt, nicht erfüllt), ermöglichen Auditberichte feingliedrige Feststellungen (erfüllt, erfüllt mit Abweichungen, nicht erfüllt).

Neben den materiellen Anforderungen eines Kriterienkatalogs treten die prozeduralen Anforderungen. Diese sind – im Sinne einer objektiven Vergleichbarkeit – mindestens genauso wichtig, da diese unter Anderem die Unabhängigkeit und Vergleichbarkeit der Feststellungen gewährleisten.

Neben die Kategorien der Zertifizierungen und Audits treten sogenannte **Reifegradmodelle**. Hierbei werden (ungeprüfte) Eigenschaften entlang eines Gradienten verortet um letztlich eine qualitative Aussage über den Prüfgegenstand zu treffen. Je höher der Reifegrad, umso höher die „Reife“, also die „Qualität“, wobei sich die Aussage auf unterschiedliche Dimensionen beziehen kann.

7 Siehe umfassend *Ingenrieth*, in Nink, StichwortKommentar Digitale Sicherheit, Zertifizierung, 2026.

3.1.2 Übertragung der Konzepte auf das Diskussionspapier

Die Wahl der konzeptionellen Ausgestaltung hängt von den erhofften Auswirkungen des Kriterienkatalogs ab:

Eine **Momentaufnahme** (etwa „‘Produktzertifizierung“) erscheint für das Ziel einer Digitalen Souveränität, die per definitionem eine Langzeitdimension und eine Zukunftsorientierung aufweist, **wenig zielführend**.

Die **Zertifizierung eines Managementprozesses** erscheint schon eher geeignet, aber weist **relevante Schwächen** auf. Dies würde genügen, soweit es Ziel des Kriterienkatalogs wäre eine „Souveränität per Checkbox“ zu erreichen. Allerdings dürfte eine solche Ausgestaltung der Intention zuwiderlaufen, einem etwaigen Verwässern des Begriffs entgegenzutreten.[8] Eine Managementprozess-Zertifizierung könnte allenfalls sachdienlich sein, soweit hierbei sehr konkrete Kriterien und Leitlinien entwickelt würden, inklusive definierter Konsequenzen und Handlungsalternativen. Eine derartige Granularität erscheint aber aufgrund der noch hoch-dynamischen Diskussionen bezüglich des Verständnisses von „Digitaler Souveränität“ höchst-herausfordernd.

Ist es Ziel des Kriterienkatalogs rückwirkend Missstände und Herausforderungen zu erkennen und somit für die Zukunft Entwicklungspotentiale aufzuzeigen und in adaptierten Kriterien nutzbar zu machen, erscheint es **zielführend, ein Audit-Programm zu entwickeln**. Audit-Programme orientieren sich eher an „Dimensionen/Objectives“ und erlauben die Ausarbeitung konkreterer interner Kriterien bezogen auf den jeweiligen konkreten Prüfgegenstand. Hierbei ist es systemimmanent, dass ein Audit Schwachstellen aufdeckt und Entwicklungspotentiale aufzeigt. Entlang dieser Erkenntnisse werden sodann die internen Kriterien beständig modifiziert und optimiert. Die hohe Individualität der internen Kriterien ermöglicht einerseits eine hohe Flexibilität und potentielle Breitenwirkung. Andererseits **erschwert es eine Vergleichbarkeit** der jeweils bewerteten, individuellen Prüfgegenstände.

Unter Berücksichtigung des erklärten Ziels, eine **Vergleichbarkeit schnell und mit verhältnismäßigem Aufwand herzustellen, erscheint ein Reifegradmodell sachdienlich**. Der Kriterienkatalog würde die bestehenden, diversen Herangehensweisen systematisieren und in eine die Vergleichbarkeit fördernde Matrix überführen. Soweit neben der Vergleichbarkeit kurz- oder mittelfristig auch eine Verlässlichkeit und Objektivität der Aussagen erzielt werden soll, **können Reifegradmodelle mit anderen Formen der Zertifizierung und Auditierung kombiniert werden**. In diesem Falle müssen alle oder einzelne Aspekte für die Erreichung eines bestimmten Reifegrads durch Prüfberichte nachgewiesen werden.

8 Siehe Kapitel 2, S. 6 Diskussionspapier.

Eine Reifegradmodell hätte zu dem den Vorteil, dass der Kriterienkatalog zumindest vorerst die **Prozeduralen Aspekte vermeiden** kann. Gerade die das Prüfverfahren betreffenden Aspekte stellen häufig einen mindestens genauso umfangreichen, wenn nicht sogar umfangreicheren Anteil der Konformitätsprogramme dar.

Empfehlung 1: Es wird empfohlen den Kriterienkatalog als Reifegradmodell auszubauen.

Das Reifegradmodell ermöglicht es die Vielzahl der sachdienlichen Maßnahmen zur Erreichung einer Digitalen Souveränität zu systematisieren. Durch ein Reifegradmodell wird eine **Bewertung einer Konformität im Sinne des „richtig / falsch" vermieden**. Insoweit besteht ein geringeres Risiko der Ablehnung durch Verantwortliche und einzelnen Sektoren, nur weil einzelne Wertungen nicht geteilt werden oder die Umsetzung dessen abgelehnt wird. Zudem sind **hohe Mitnahme-Effekte** zu erwarten. Die Verantwortlichen für die Implementierung und Steuerung werden nicht dem unnötigen Eindruck eigener Schlechtleistung unterworfen, während ihnen zugleich – aufgrund der möglichen Feingliedrigkeit der Aspekte – unmittelbare und leicht implementierbare Verbesserungen an die Hand gegeben werden. Gerade in hoch-interdependenten Themen, wie der Digitalen Souveränität, ist ein Handlungshemmnis die vermeintliche „Größe" der zu bewältigen Aufgabe. Eine **durch das Reifegrad-Modell angeleitete Aufteilung in (kleinst-)Projekte kann derartige Hemmnisse bei den Verantwortlichen überwinden**. Zugleich erleichtert es die Kommunikation, Präsentation und Finanzierung im Rahmen von internen Freigabeprozessen, da die Maßnahmen und die Auswirkungen greifbarer werden.

Empfehlung 2: Es wird empfohlen den Kriterienkatalog als offenes Reifegradmodell auszugestalten.[9]

Obgleich sich in vielen Bereichen eine Dreistufigkeit (low/basic, essential, high) etabliert, wird von einer derartigen Ausgestaltung im Reifegradmodell für Digitale Souveränität abgeraten.

Der Begriff der Digitalen Souveränität ist höchst-dynamisch. Die in Rede stehenden Maßnahmen und Kriterien sind interdependent und somit von unterschiedlichen Interessen geleitet. Es wird daher bereits eine Herausforderung darstellen, je Dimension einzelne Umstände hierarchisch in einen Reifegradgradienten zu überführen. Müssten sich diese Aspekte zudem in **definierte Stufen eingliedern, droht dies erheblichen**

9 „Offene Reifegradmodelle" zeichnen sich dadurch aus, dass je Dimension/Objective unterschiedlich viele Aspekten existieren können und sich diese Aspekte nicht in ein vordefiniertes Schema von Reifestufen eingliedern müssen; vgl. exemplarisch das „Reifegradmodell zur Abbildung von technisch-organisatorischen Maßnahmen bei der Auftragsverarbeitung", entwickelt und herausgegeben durch bitkom in 2024. Das Modell zeigt zudem auch auf, wie externe Validierungen in ein Reifegradmodell eingebunden werden können. abrufbar unter https://www.bitkom.org/sites/main/files/2024-11/241104-LF-Datenschutz-Reifegradmodell-Bitkom.pdf.

Blockade-Haltungen zu begegnen. Derartige Stufen würden letztlich den Vorteil eines an sich wertungsneutralen Reifegrad-Modells zu Nichte machen. Vielmehr würde der **Eindruck** entstehen, dass durch bestimmte Reifegradstufen bereits **korrespondierende „Konformitäten“** erreicht seien. Es ist aus der Erfahrung mit ähnlich gelagerten Vorhaben zu erwarten, dass **Stakeholder auf solche Automatismen hinwirken** würden.

Im Ergebnis würden bei einer vorgegebenen (Drei-)Stufigkeit Chancen verloren gehen, jedenfalls (1) eine ergebnisoffene Sammlung von Maßnahmen und (2) ein Fokus auf Effektivität und objektive Vergleichbarkeit.

Stakeholder werden im Falle eines engen und zu erwartenden Konformitätskorsetts nicht gewillt sein, ergebnisoffen Maßnahmen vorzutragen. Diese Zurückhaltung begründet sich etwa weil einzelne Maßnahme eventuell aus anderen Überlegungen als der Digitalen Souveränität umstritten sind[10], (hohe oder anderenfalls entfallene) Aufwände bedeuten würden, oder lediglich in besonderen Konstellationen[11] erforderlich scheinen. Allerdings ist diese **Offenheit gerade die Intention eines Reifegrad-Modells**. Die Aspekte werden entlang eines Gradienten verortet entsprechend der erwarteten positiven Auswirkungen. Es ist dann Aufgabe derjenigen, die den **konkreten Einsatzzweck** kennen, die erforderliche „Reife“ je Dimension anhand der **eigenen Risiko- und Anforderungsanalyse** zu definieren. Da es gerade keinen Automatismus zur Konformität oder zu einer Implementierungspflicht gibt, können Reifegradmodelle ohne unmittelbare Konsequenzen auch höchst seltene, ausgefallene oder aufwändige Maßnahmen aufnehmen und somit den (gedanklichen und entwicklungstechnischen) Rahmen und Ausblick auf mögliche künftige Optionen aufzeigen.

Fehlt eine solche Ergebnisoffenheit können andere Überlegungen überwiegen, die dazu führen könnten, dass am Ende lediglich die Erreichbarkeit einer bestimmten **„Reifegradstufe“ durch die Mehrheit der etablierten Stakeholder** garantiert ist. Diese könnten sodann leicht die relevante Stufe erreichen, und im Falle etwaiger Automatismen resultiert der Kriterienkatalog dann in einer möglichen **Verwässerung des Begriffs der Digitalen Souveränität**. Denn in diesem Falle stünde nicht mehr die im konkreten Anwendungsfall erforderliche Effektivität im Fokus, sondern ausschließlich die Absicherung der eigenen Verantwortlichkeiten durch **Nachweise der richtigen „Checkbox“.**

10 Etwa, weil diese nicht von eigenen Produkten bereits umgesetzt sind, weil diese möglicherweise Konkurrenten eher befähigt, oder in Widerspruch zu bisherigen politischen oder werblichen Aussagen stehen.

11 Z.B. in höchst-sensiblen Kontexten der nationalen Sicherheit.

3.2 Klarheit bezüglich des Gegenstands der Betrachtung

Derzeit ist nicht klar, was Gegenstand der Betrachtung (**Prüfgegenstand**) des Kriterienkatalogs sein soll. Einerseits weist das Diskussionspapier daraufhin, dass gerade nicht einzelne Produkte oder Systeme betrachtet werden sollen, sondern die Öffentliche Verwaltung als Ganzes, inklusive des gesamten digitalen Stacks.

Gleichzeitig soll die Öffentliche Verwaltung (durch den Kriterienkatalog) in die Lage versetzt werden, IT-Lösungen, Komponenten und Anbieter flexibel auszuwählen und bei Bedarf mit vertretbarem Aufwand zu wechseln.[12]

Hierbei sollte zunächst klar sein, was die Zielsetzung des Kriterienkatalogs ist. Es ist auch vorstellbar, dass es mehrere Zielsetzungen bereits hinsichtlich des Prüfgegenstands gibt. In diesem Falle sollte der Kriterienkatalog in unterschiedliche Kataloge bzw. Sub-Kataloge aufgeteilt werden.

Empfehlung: Es wird empfohlen, die Zielsetzung des Kriterienkatalogs zu klären und die Dimensionen und Kriterien streng anhand dieser Zielsetzung auszugestalten.

> Bestehen Unwägbarkeiten hinsichtlich der Zielsetzung wird dies die weitere Entwicklung verzögern, da unterschiedliche Stakeholder die Unwägbarkeiten nutzen könnten, um deren eigenen Interessen zu sichern.

3.3 Existenz von und erforderliche Klarheit bezüglich der Kriterien

Bisher weist das Diskussionspapier lediglich Dimensionen, allenfalls Objectives auf. Konkrete Kriterien sind nicht ersichtlich, geschweige denn Empfehlungen oder Beispiele zu den Kriterien.[13]

Inwieweit die konkreten Dimensionen bzw. Objectives geeignet sind bzw. ergänzt werden müssten, hängt von dem beabsichtigten Prüfgegenstand ab. Im weiteren wird als Prüfgegenstand die Öffentliche Verwaltung beziehungsweise derer Organisationseinheiten vorausgesetzt.

Empfehlung: Für eine objektive und vergleichbare Erfassung der Umstände müssten die Dimensionen und die Objectives in konkrete Kriterien überführt werden. Aufgrund der hohen Dynamik sollte hierbei insbesondere auch auf ergänzende Erläuterungen zurückgegriffen werden, inklusive Beispielen und Empfehlungen.

12 Kapitel 3, S. 9 Diskussionspapier.

13 Weitergehend zu den Begrifflichkeiten *Ingenrieth*, in Nink, StichwortKommentar Digitale Sicherheit, Zertifizierung, 2026.

3.4 Synergiepotentiale zu anderen Souveränitätskriterien

Es ist zu begrüßen, dass das Diskussionspapier die Kriterien des European Cloud Sovereignty Framework (**EU CSF**)[14] sowie die BSI Criteria Enabling Cloud Computing Autonomy (**BSI C3A**)[15] in Bezug nimmt. Generell sollte sichergestellt werden, dass eine sachdienliche Kompatibilität aufrecht erhalten wird.

Insoweit ist ebenfalls auf den Prüfgegenstand abzustellen. Das EU CSF und die BSI C3A-Kriterien stellen im Wesentlichen die jeweiligen Digitalen Dienste in den Fokus. Das Diskussionspapier scheint aber sehr bewusst einen anderen Fokus setzen zu wollen. Soweit die **Fähigkeiten und Implementierungsfortschritte der Öffentlichen Verwaltung** betrachtet werden sollen, erscheinen das EU CSF und die BSI C3A-Kriterien nicht geeignet.

Es erscheint indessen **höchst sachdienlich, mit dem Diskussionspapier einen anderen Fokus zu setzen**. Nicht alle Fachverfahren und digitalen Prozesse, inklusive der damit verbundenen Datenverarbeitung, Speicher- und Netzwerkinfrastruktur, sind durch oder müssen durch Cloud-Dienste realisiert werden. Jedwede **Prozesse und Infrastruktur, die nicht über Cloud-Dienste realisiert werden, verblieben somit in einem „Blinden Fleck“**. Hierzu zählen auch etwaige (mobile) Endgeräte und deren Firmware, Betriebssysteme und sonstiger Software. Auch digitale Gebäude- und Bereichssicherungssysteme sind möglicherweise digitale Verfahren. Diese kurze Darstellung zeigt bereits, warum die Kriterien-Kataloge mit reinem Cloud-Fokus einer Ergänzung bedürfen.

Zugleich erscheint es nicht sachdienlich, in angemessener Zeit, einen Rundumschlag zu realisieren. Vielmehr wirkt es förderlicher und effizienter, die Zielrichtungen der Prüfgegenstände strikt zu trennen und hierdurch ein **Souveränitäts-Netz** zu spannen. Einzelne Dimensionen können sich somit sowohl **horizontal ergänzen, als auch vertikal aufeinander aufbauen**.

Hierdurch ergeben sich allgemeine Anforderungen an die Informationsbeschaffung, Dokumentation sowie hinsichtlich der Fertigkeiten der Öffentlichen Verwaltung. Hierbei umfassen die Fertigkeiten die finanziellen und sachlichen Ressourcen, und das notwendige Fachwissen die sachlichen Ressourcen sachdienlich einzusetzen und eine **angemessene und unabhängige Risikoanalyse** durchführen zu können.

14 https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en?file-name=Cloud-Sovereignty-Framework.pdf

15 Download at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf; First analysis, e.g. *Ingenrieth*, BSI C3A:v1 on Cloud Autonomy published by Federal Office for Information Security : https://ingenrieth-online.de/de/aktuelles/detail/bsi-c3av1-on-cloud-autonomy-published-by-federal-office-for-information-security

Empfehlung 1: Es sollte deutlich(er) herausgearbeitet werden, wie durch den Kriterienkatalog die Aspekte der Digitalen Souveränität ergänzt werden.

Empfehlung 2: Es sollte auf unnötige Redundanzen verzichtet werden, da diese letztlich zu einer vermeidbaren Hürde bei der Implementierung führen. Redundanzen lösen – auch ungewollt – Auslegungskonflikte aus, insbesondere soweit die Redundanz nicht wort- und kontextidentisch ist.

Empfehlung 3: Wenn und soweit Elemente des EU CSG oder der BSI C3A für förderlich aus Sicht des Diskussionspapiers erachtet werden, und eine Übernahme der Inhalte zielführend und nicht vermeidbar ist, sollte allenfalls ein (statischer) Verweis auf die jeweiligen Kriterien erfolgen und diese somit inkorporiert werden.

Empfehlung 4: Soweit Informationen bereits aufgrund anderer Kriterienkataloge objektiv und sachdienlich erfasst werden, etwa Lieferketten (Vendor Management), oder anwendbare Jurisdiktionen inklusive der implementierten Mitigationsmaßnahmen, so sollten die Kriterien des Diskussionspapiers die Öffentliche Verwaltung dahingehend ertüchtigen und messen, ob diese bereits bestehenden Kriterienkataloge bekannt und verwendet werden. Dies kann auch eine kritische Auseinandersetzung mit den jeweiligen Schwächen der existierenden Kriterienkataloge sein, mit der Folge, dass die Öffentliche Verwaltung diese Schwächen durch eigene, ergänzende Maßnahmen neutralisiert.

3.5 Risikobetrachtung

Positiv ist hervorzuheben, dass das Diskussionspapier die Diversität der zugrundeliegenden Sachverhalte anerkennt. Soll die Effektivität in den Fokus gestellt werden, erscheint eine konzeptionell individualisierte Vorgehensweise nachvollziehbar.

Es ist zu beachten, dass eine **konzeptionelle Individualisierung** trotzdem einen **hohen Grad an Synergien** ermöglicht. Hierzu sollte parallel zu den Kriterien ein interner Austausch der Verantwortlichen in der Öffentlichen Verwaltung etabliert werden. Ein solcher Austausch kann – und sollte – die jeweils getroffenen Maßnahmen dokumentieren und für andere zugänglich machen. Die so gewonnenen „good practices“ ermöglichen letztlich einen hohen Effizienzgewinn auf Basis einer de facto Standardisierung, erhält aber den hohen Grad der individuellen Flexibilität.

Ein zu hoher **– zentral vorgegebener – Grad der Standardisierung könnte der Digitalen Souveränität auch zuwiderlaufen**. Souveränität ist in erster Linie die Fähigkeit, eigenständig in Kenntnis der Umstände entscheiden zu können. Faktische Abhängigkeiten entstehen insbesondere, wenn einzelne Lösungen und Maßnahmen auf Ebene der Implementierung so dominant werden, dass diese als „too big/important to fail“ gelten. Eine **zentrale**

Standardisierung von Maßnahmen fördert derartige Dominanzen. Im Ergebnis könnte somit eine Abhängigkeit A lediglich in eine Abhängigkeit B verlagert werden. Die Möglichkeit individuelle Maßnahmen implementieren zu können, erscheint daher ein zentraler Aspekt, die notwendige Diversität der getroffenen Maßnahmen zu erreichen. Eine **Diversität der getroffenen Maßnahmen** ermöglicht zudem auch einen **Vergleich der Maßnahmen** und der sich aus der Maßnahme ergebenden **Potentiale**. Diese vielfältigen Erfahrungen können wiederum für die Weiterentwicklung und Optimierung der individuellen Maßnahmen genutzt werden.

Empfehlung 1: Die Risikobetrachtung sollte eine eigene Dimension darstellen.

Es ist zwar zutreffend, dass die Risiken sich über die jeweiligen Dimensionen – auch – als Querschnittsmaterie realisieren, jedoch existieren vorgelagert wichtige Aspekte, die sichergestellt werden sollten. Dies betrifft etwa die Fähigkeiten und Maßnahmen, Risiken erkennen und bewerten zu können, die etwaige kaskadierte kollateral-Folgen erkennen zu können oder eben die (un-)mittelbaren Auswirkungen durch Sicherungsmaßnahmen in nachgelagerten Verfahren adressieren zu können.

Empfehlung 2: Die Möglichkeit individueller Maßnahmen sollte aufrecht erhalten werden.

Die hierdurch mögliche Diversität erhöht den Erfahrungsgewinn, der wiederum in alle Maßnahmen ausstrahlt. Zudem birgt eine zu große Standardisierung das inhärente Risiko, dass am Ende eine Abhängigkeit von der standardisierten Maßnahme etabliert wird.[16]

16 Sicherheitstechnische Betrachtungen bleiben vorliegend außer Acht. Standardisierung ist stets auch aus einer sicherheitstechnischen Betrachtung in einem Spannungsfeld: einerseits erleichtert die Standardisierung die Aufrechterhaltung eines hohen Niveaus in der Fläche; andererseits vergrößert Standardisierung auch den Angriffsvektor, soweit eine Lücke in der Sicherheitsarchitektur erkannt wird, da Angreifer diese nun flächendeckend vorfinden.

4 Spezifische Anmerkungen

Spezifische Anmerkungen beziehen sich auf die Elemente der jeweiligen Dimensionen, soweit dies nicht bereits Gegenstand der allgemeinen Betrachtung war.

Hierbei sind zwei Prämissen besonders wichtig:

- entwickelt sich das Diskussionspapier zu einem offenen Reifegradmodell, stellen die zu entwickelnden Kriterien lediglich individuelle Aspekte der Reife dar;
- verbleibt das Diskussionspapier in einem Konzept der (binären) Konformität, so sollten die Kriterien in ihrer Struktur optimiert und weiter systematisiert werden.

Hierbei sind auch Kombinationen möglich, wobei es oberste Priorität sein muss, die Zielsetzung des Kriterienkatalogs zu schärfen.

4.1 Dimension A

Die Dimension A erscheint sachdienlich und die primäre Dimension zur Ertüchtigung der Öffentlichen Verwaltung.

Es erscheint sachdienlich, die weiteren – teils technischen – Dimensionen stärker an die Dimension A anzubinden.

Der Prüfgegenstand ist bisher unklar. Die Digitale Souveränität der Verwaltung für den gesamten Stack inkludiert sowohl die technische Dimension als auch die organisatorische Dimension.

Wie bereits zuvor erwähnt, erscheint der Kriterienkatalog alle Dimensionen und Aspekte des digitalen Stacks zu umfassen. Sowohl die Erstellung, als auch die weitere Pflege würde enorme Ressourcen beanspruchen. Die Vermischung der Prüfgegenstände würde zudem zu einer Verwässerung der Zielsetzungen führen, da neben einem Fokus auf Digitale Souveränität andere **politische und wirtschaftliche Überlegungen** die Entwicklung beeinflussen könnten.

Eine solche **Verwässerung und Ablenkung** kann **ergebnisorientierter begegnet** werden, wenn der **Prüfgegenstand klar und fokussiert** ist.

Insoweit ist es unbenommen, dass auch technische Aspekte entlang des digitalen Stacks der Öffentlichen Verwaltung betrachtet werden müssen. Die jetzige Ausgestaltung und Zielsetzung des Diskussionspapiers scheint es aber aufzudrängen, diese technische Betrachtung auszulagern in eigene Kriterienkataloge.

Konzeptionell würde somit die Dimension A bedeuten:

- Aufbau und Erhalt von **(Fach-)Expertise**
- Aufbau und Erhalt von **Erkenntnis- und Dokumentationsverfahren**
- Aufbau und Erhalt von **Evaluations- und Reaktionsmechanismen**
- Aufbau und Erhalt von **Beschaffungs- und Entscheidungsstrukturen** zum Aufbau und Erhalt digitaler Souveränität
- Aufbau und Erhalt von (internen) **Austauschplattformen** zur Entwicklung und Weitergabe von „good practises“ im Rahmen genutzter Mechanismen
- Aufbau und Erhalt übergeordneter **Transparenzstrukturen** zur Vermeidung ungewollter und indirekter Abhängigkeiten
- Aufbau und Erhalt von **Experimentalverfahren und Sprint-Umgebungen**

Soweit Fachexpertise betroffen ist, kann diese in unterschiedlicher Granularität erforderlich sein und sollte somit auch graduell ertüchtigt werden. Die notwendige Fachexpertise reicht von verständigem Bewusstsein bis hin zu der Fähigkeit, eigene (technische) Elemente eigenständig und autonom entwickeln zu können. **Entlang dieses Gradienten können auch ergänzende Kriterienkataloge unterstützen**. Insoweit ist es Teil der Ertüchtigung der Öffentlichen Verwaltung, diese Kriterienkataloge bekannt zu machen, die Vor- und Nachteile zu kennen, und letztlich in angemessenen Umfang bei eigenen Entscheidungen und der Beschaffung zu berücksichtigen.[17]

Insbesondere erscheint neben der individuellen Fachexpertise eine **Überwindung der Silo-Strukturen** erforderlich. Einerseits beschleunigt ein Fachaustausch die Ertüchtigung, da die Fachbereiche aus wechselseitigen Erfahrungen eigene Entscheidungen ableiten können. Es kann von einem hohen Synergiepotential ausgegangen werden. Zudem kann hierdurch vermieden werden, dass sich **(ungewollt und indirekt) entlang des digitalen Stacks einzelne digitale Dienste verdichten** und somit zu einer unbeabsichtigten, **schleichenden Abhängigkeit** führen.

Diese **Synergien** gehen einher mit der **positiven Konnotation**, dass auch fremde Fachbereiche sachdienliche und ggf. optimierte Mechanismen etabliert haben können, deren **Übertragung auf die eigenen Fachverfahren** förderlich ist. Hierzu erscheint es sachdienlich, die Gemeinsamkeiten der Verfahren in den Mittelpunkt der Betrachtung zu stellen, und auf deren Basis modular die Besonderheiten zu adressieren. Hierzu erscheint es konzeptionell förderlich, dass

17 Zu relevanten Fragen bei der Bewertung und Evaluation von (externen) Prüfverfahren, siehe auch *Ingenrieth*, in Nink, StichwortKommentar Digitale Sicherheit, Zertifizierung, 2026. Zu relevanten Fragen wie die Unabhängigkeit bzw. das Gleichgewicht der berücksichtigten Interessen ermittelt werden kann, siehe etwa *Ingenrieth*, in Nink, StichwortKommentar Digitale Sicherheit, Ko-Regulierung, 2026.

auch die **Vorteile einer dynamischen Entwicklung** in den Vordergrund gestellt werden. Im Falle einer **sachdienlichen Trennung der Hintergrundprozesse und Hintergrundsysteme von deren Bedienungsoberflächen** führt eine Umstellung dieser Hintergrundprozesse zu geringen bis keinen Schulungsbedarfen der Endnutzer*Innen.

Die obig genannten Aspekte der Dimension A können zudem sehr gut in Reifegraden dargestellt werden.

Empfehlung 1: Es wird empfohlen, die Dimension A stärker auf die nicht-technischen Aspekte einer organisatorischen Ertüchtigung zu fokussieren, und dabei die Erkenntnisse der weiteren Dimensionen nutzbar zu machen.

Empfehlung 2: Es wird empfohlen, etwaige technische Aspekte entweder auf Basis der bereits entwickelten weiteren Kriterienkataloge zu inkludieren, oder in eigene, noch zu entwickelnde Kriterienkataloge auszulagern und hierdurch die Zielsetzung des Diskussionspapiers zu schärfen, und somit schnellere, und nachhaltigere Effekte zu erzielen.

4.2 Dimension B

Insgesamt wirkt diese Dimension **teils redundant und in sich unschlüssig**, obgleich die einzelnen Elemente einer Digitalen Souveränität zuträglich sein können.

So erscheint „Transparenz und Dokumentation“ Redundant zur Dimension A der IT-Governance und des Managements. Die Dokumentation und Transparenz ist hierzu eine *conditio sine qua non*. Dies gilt auch für ein Risikomanagement. Ohne Kenntnis der Umstände ist ein Risikomanagement nicht zielführend. Dies inkludiert auch die Dokumentation über getroffene Entscheidungen und die damit verbundenen, akzeptierten Risiken. Denn nur so können künftige Entscheidungen nachhaltig und verständig getroffen werden.

Soweit Dimension B technische Aspekte betrifft, sollte dies in eine Fähigkeits- und Berücksichtungsmatrix überführt werden, während die eigentlichen technischen Aspekte in kontextualisierte Kriterienkataloge überführt werden.

Hierbei ist zu beachten, dass die Fähigkeits- und Berücksichtigungsmatrix sehr gut in ein Reifegradmodell überführt werden kann. Technische Aspekte, je nach deren Detailgrad, erscheinen sachdienlicher in konkreten Konformitätsprogrammen. Obgleich auch in diesem Kontext sind Reifegrade vorstellbar.

Soweit auf **Standards und Schnittstellen** abgestellt wird, sollte der Kriterienkatalog klarstellen, was hierdurch adressiert werden soll. Positiv ist sicherlich, wenn die Öffentliche Verwaltung deren **digitale Verfahren stärker in Modulen organisiert** und den **Austausch von Inhalten stärker über Schnittstellen** realisiert. Im Sinne der Organisations- und

(Weiter-)Entwicklungskompetenzen erscheint ein **Fokus auf Open Source nahe liegend**. Hierbei sollte aber unterschieden werden, was durch Open Source tatsächlich erreicht werden kann. **Automatismen hinsichtlich der positiven Bewertung von Open Source sollten vermieden werden**. Ein „öffentlich verfügbarer Source Code“ bedeutet nicht notwendigerweise, volle Nutzungs- und Verwertungsrechte. Umgekehrt verlangen umfassende Nutzungs- und Verwertungsrechte nicht die Veröffentlichung des Source Codes.

Empfehlung: Redundanzen reduzieren, Zielsetzung der Dimension schärfen, und im Ergebnis zunächst den Fokus auf eine referenzielle Inklusion in Dimension A legen.

4.3 Dimension C

Diese Dimension beschäftigt sich mit der Perspektive „Daten“. Auch hier sind teilweise Redundanzen erkennbar.

Die Datenstruktur ist eng mit der Entwicklung und Ausgestaltung von (Daten-)Schnittstellen verbunden.

Die Datensicherheit wird in der Regel durch IT-Sicherheitskriterien adressiert. Insoweit sollte klargestellt werden, **an welchen Stellen die durch das Diskussionspapier angedachten Kriterien gegenüber den etablierten IT-Sicherheitsstandards einen Mehrwert bieten**. Denkbar erscheint auch hier ein Rückgriff auf die Dimension A dahingehend, dass die Verantwortlichen in der Öffentlichen Verwaltung ertüchtigt werden, die etablierten Standards sowohl zu kennen, als auch deren Aussagen in den eigenen Entscheidungen verständig einfließen zu lassen.

Soweit **Datenlokation** betroffen ist, sollte klargestellt werden, dass bei einer Verarbeitung von Daten in öffentlichen Netzen, bzw. in Netzen, die eine Anbindung an öffentliche Netze haben, die **Lokation nur eine sekundäre Sicherheit** bietet. Eine Verarbeitung „in Europa“ garantiert nicht, dass die hiesigen Rechtsnormen eingehalten werden. Es erleichtert allenfalls deren Durchsetzung. Zugleich ist eine Datenlokation außerhalb von Europa nicht gleichzusetzen mit einem garantierten Missbrauch der Daten durch Dritte.

Es sollte hierbei eine **differenzierte und zielorientierte Betrachtung** stattfinden. Eine räumliche Konzentration der digitalen Dienste erhöht das Risiko eines Single-Point-Of-Failures. Das gleiche gilt für die Nationalitäten und Wohnsitze der mit der Datenverarbeitung betrauten Personen. Beide Aspekte sind ein **ungeeigneter Proxy und eine Verwässerung einer effektiven Risikomitigation**. Das Risiko ist der Single-Point-Of-Failure. Der Proxy verleitet zu einer Risiko-Ignoranz aufgrund einer positiven „Checkbox“.[18] Die Intention des Diskussionspapiers,

18 Siehe hierzu etwa die initiale Analyse der BSI C3A Kriterien, *Ingenrieth*, BSI C3A:v1 on Cloud Autonomy published by Federal Office for Information Security, https://ingenrieth-online.de/de/aktuelles/detail/bsi-c3av1-on-cloud-autonomy-published-by-federal-office-for-information-security.

derartigen **Verwässerungen und Fehlanreizen entgegenzuwirken,** sollte durch eine sachdienliche Schärfung des Regelungsziels und der damit verbundenen Kriterien und Erwartungen befördert und effektuiert werden.

Empfehlung: Redundanzen reduzieren, Zielsetzung der Dimension schärfen, und im Ergebnis zunächst den Fokus auf eine referenzielle Inklusion in Dimension A legen.

4.4 Dimension D

Hierbei sind einige Redundanzen mit den weiteren Dimensionen festzustellen.

Datenschutz inkludiert Datensicherheit und IT-Sicherheit, wobei hierdurch auch zwingend Überlegungen im Bereich des Business Continuity Managements und sowie der Sicherheit und Compliance im Betrieb anzustellen sind.

Denkbar erscheint eine **Schärfung der Dimension**, oder eine **referenzielle Inklusion** in andere Dimensionen. Letzteres wäre dem primären Zweck des Diskussionspapier förderlich und könnte in ein Reifegradmodell überführt werden. Die weiteren, detaillierten Anforderungen wären in diesem Fall in ergänzenden Kriterienkatalogen und Konformitätsbewertungsprogrammen zu etablieren und zu pflegen.

Empfehlung: Redundanzen reduzieren, Zielsetzung der Dimension schärfen, und im Ergebnis zunächst den Fokus auf eine referenzielle Inklusion in Dimension A legen.

5 Fazit

Das Diskussionspapier liefert einen guten Überblick über den aktuellen Sachstand bezüglich der „Digitalen Souveränität“. Die Definition des Begriffs ist nach wie vor nicht abgeschlossen und somit ist auch eine Entwicklung von klaren Kriterien schwierig.

Der **Dynamik des Themenfelds** geschuldet, erscheint es somit sachdienlich, zunächst eine **ergebnisoffene und wertungsneutrale Matrix** zu entwickeln, etwa in Form eines Reifegradmodells.

Aus dem **Reifegradmodell** können sodann konkrete Anforderungen (Reifegrade) für bestimmte **horizontale oder vertikale Anwendungsfälle** extrahiert werden.

Wichtig erscheint, dass sich der zu entwickelnde Kriterienkatalog einerseits in die Logik der bereits anderweitig ausgearbeiteten Kriterienkataloge einbinden lässt. Andererseits erscheint es sachdienlich, die **Effektivität und Individualität** aufrecht zu erhalten.

Ebenfalls erscheint ein konkreter Bedarf gegeben, da die bisherigen Kriterienkataloge entweder nur einen Ausschnitt der digitalen Dienste bzw. des digitalen Stacks der Öffentlichen Verwaltung abbilden; oder weil die bisherigen Kriterienkataloge eine Verwässerung der Effektivität und der eigenen, verständigen Entscheidung befördern könnten.

Hierbei sollte insbesondere darauf geachtet werden, **Fehlanreize und Fehlwirkungen zu vermeiden**. Zugleich sollte vermieden werden, Verantwortliche in der Verwaltung dem Anschein anzusetzen, dass diese bisher ausschließlich fehlerhafte Entscheidungen getroffen haben. Stattdessen sollten die Kriterien und das empfohlene Format eines offenen Reifegradmodells eine **selbstkritische aber ansonsten wertungsneutrale Auseinandersetzung mit dem Status Quo** ermöglichen und zugleich **niederschwellige Entwicklungs- und Optimierungspotentiale aufzeigen**. Eine **konsistente und kontinuierliche Berücksichtigung** der Entscheidungsdimension „Digitale Souveränität“ wird im Ergebnis **nachhaltigere und zeitnähere Effekte** begründen können, als medial-politische Großprojekte. Einerseits ist die Finanzierung derartiger **Großprojekte schwierige**r, andererseits ist die Umsetzung von Großprojekten **vergleichsweise träge** und daher dem Risiko ausgesetzt, dass sich die Anforderungen im hoch-dynamischen Themenfeld der Digitalen Souveränität bereits verändert haben, bevor das Großprojekt überhaupt Wirkung entfalten kann.

Öffentliche Konsultation - Diskussionspapier

Kriterien für Digitale Souveränität – aus messbar wird machbar

Mai 2026

Rechtsanwalt Frank Ingenrieth, LL.M.