HOHEIT ÜBER DEN CODE

Standard des digitalen öffentlichen Rechts

INSTITUTE FOR DIGITAL SOCIETY & FUTURE PUBLIC LAW

KONSULTATIONSENTWURF V1.0 – 28. SEPTEMBER 2026

STATUS DIESES DOKUMENTS

Verfahrensstand. Konsultationsentwurf, Version 1.0, vom 28. September 2026. Registereintrag: wird bei Eröffnung der Konsultation vergeben.

Herausgebende Stelle. Herausgegeben vom EPLO Institute for Digital Society and Future Public Law.

Rechtswirkung. Der Standard ist Soft Law. Er ist rechtlich nicht verbindlich, es sei denn, eine zuständige Behörde verleiht ihm durch ein eigenes Instrument Wirkung.

Konsultation. Öffentliche Konsultation von mindestens sechzig (60) Tagen. Zur Stellungnahme eingeladen sind öffentliche Institutionen, Aufsichtsstellen, Gerichte und Ombudsstellen, Forschende, die Zivilgesellschaft und Lieferanten. Stellungnahmen werden unter dem Namen der Verfasserin oder des Verfassers eingereicht und mit diesem Namen veröffentlicht; anonyme und vertrauliche Stellungnahmen werden nicht angenommen.

ENTWURF

Einleitung

Öffentliche Gewalt wird heute regelmäßig durch digitale Systeme ausgeübt: durch Scoring-Modelle, die auswählen, gegen wen eine Behörde ermittelt, durch digitale Brieftaschen, die den Zugang zu grenzüberschreitenden Diensten kontrollieren, und durch Datenplattformen, die prägen, wie Krankenhäuser ihre Kapazitäten zuteilen. Das Fachrecht prüft jedes dieser Systeme ausschnittsweise. Das Datenschutzrecht fragt, ob personenbezogene Daten rechtmäßig verarbeitet werden, das KI-Recht, ob ein Modell die risikobasierten Anforderungen erfüllt, denen es unterliegt, und das Cybersicherheitsrecht, ob Vorfälle bewältigt und gemeldet werden. Keine fachrechtliche Regelung stellt die übergreifende Frage, die dieser Standard behandelt: Bewahrt die verantwortliche öffentliche Institution die rechtliche und praktische Fähigkeit, das digitale Arrangement, durch das sie öffentliche Gewalt ausübt, zu verstehen, zu lenken, zu prüfen, zu korrigieren und erforderlichenfalls zu beenden?

Der Staat bewahrt die Hoheit über den Code nicht schon dadurch, dass er über einen Vertrag, eine Richtlinie oder eine Plattform verfügt. Er bewahrt sie nur, wenn die rechtmäßige öffentliche Gewalt nachweislich in der Lage bleibt, die technischen und soziotechnischen Arrangements, durch die eine öffentliche Aufgabe wahrgenommen wird, zu verstehen, zu lenken, zu prüfen, zu korrigieren, ihren Mängeln abzuhelfen, sie aufrechtzuerhalten und erforderlichenfalls aus ihnen auszusteigen. Hoheit über den Code wird nachgewiesen, nicht behauptet.

Der Standard gliedert sich in vier Teile. Teil I (Normativer Kern) enthält die Kernanforderung, die elf Grundsätze, die zehn bewahrten Fähigkeiten sowie die grundlegenden Tests und Begriffe. Teil II (Methode) regelt die Folgenabschätzung im digitalen öffentlichen Recht, die maßgebliche Methode des Standards, mit der geprüft wird, ob der Normative Kern bei der jeweiligen öffentlichen Aufgabe erfüllt ist. Teil III (Anwendung) legt fest, wie der Standard verwendet wird: die Verwendungsarten, die Akte der digitalen öffentlichen Aufgabe, die drei Prüfstufen und ihre Feststellungsberichte, die Formen, in denen eine zuständige Behörde dem Standard Wirkung verleihen kann, und sein Verhältnis zu anderen Instrumenten. Teil IV (Pflege des Standards und Umsetzung durch Soft Law) erläutert, wie der Standard zur Konsultation gestellt, angenommen, geändert und umgesetzt wird.

ENTWURF

Teil I – Normativer Kern

I.1 Zweck und Rechtsnatur

I.1.1 „Hoheit über den Code: Standard des digitalen öffentlichen Rechts“ (Power over Code; im Folgenden „der Standard“) legt die Mindestbedingungen fest, die erfüllt bleiben müssen, wann immer eine öffentliche Aufgabe durch digitale Systeme wahrgenommen, vermittelt, begrenzt, priorisiert oder wesentlich geprägt wird.

I.1.2 Der Standard ist ein rechtlicher Standard: ein kohärenter Bestand normativer Anforderungen samt einer maßgeblichen Methode zu ihrer Anwendung, der darauf angelegt ist, eine einheitliche Anwendung über Institutionen und Rechtsordnungen hinweg zu sichern. Seinen Inhalt schöpft er aus dem Verfassungsrecht, dem Verwaltungsrecht, den Menschenrechten und dem Fachrecht, die die öffentliche Gewalt bereits binden. Er begründet keine neuen materiellen Rechte und verdrängt nicht das anwendbare Recht, das Inhalt und Durchsetzbarkeit jeder Anforderung in der jeweiligen Rechtsordnung bestimmt.

I.1.3 Der Standard gilt für digital vermittelte öffentliche Aufgaben, die den Test des funktionalen Anwendungsbereichs (I.8.1) bestehen, unabhängig davon, ob die Aufgabe von einer öffentlichen Stelle oder von einem in ihrem Auftrag handelnden privaten Akteur wahrgenommen wird.

I.2 Normative Formulierungen

I.2.1 „Muss“ kennzeichnet entweder eine methodische Voraussetzung für eine vertretbare Schlussfolgerung nach dem Standard oder eine Pflicht, die das anwendbare Recht begründet. Jede Akte der digitalen öffentlichen Aufgabe gibt an, welcher dieser beiden Gründe vorliegt. Ist eine „Muss“-Anforderung nicht erfüllt, ist die betreffende Entscheidungskategorie gesperrt.

I.2.2 „Soll“ drückt eine nachdrückliche Erwartung des Standards aus, von der eine Institution nur mit einer dokumentierten und begründeten Rechtfertigung abweichen kann.

I.2.3 „Kann“ bezeichnet eine zulässige Möglichkeit.

I.2.4 Ein methodischer Mangel nach dem Standard ist für sich genommen keine gerichtliche Feststellung der Rechtswidrigkeit. Ebenso wenig lässt die Entscheidung, den Standard nicht anzuwenden, eine bestehende Rechtspflicht einer Institution entfallen.

I.3 Begriffsbestimmungen

I.3.1 Digitales öffentliches Recht ist das Rechtsgebiet, das sich mit der rechtlichen Konstituierung, der Ausübung, der Vermittlung und der Kontrolle öffentlicher Gewalt unter Bedingungen digitaler Abhängigkeit befasst.

I.3.2 Code bezeichnet die technisch formalisierten und operativ wirksamen Arrangements, durch die ein digitales System eine öffentliche Aufgabe wahrnimmt, vermittelt, begrenzt, priorisiert oder in sonstiger Weise wesentlich prägt. Er umfasst Software-Quellcode und ausführbaren Code; Algorithmen, Rechenregeln, Entscheidungsmodelle und KI-Modelle; Systemkonfigurationen, Schwellenwerte,

ENTWURF

Gewichte, Parameter und Voreinstellungen; Datenmodelle, Schemata, Klassifikationen sowie Trainings-, Test-, Referenz- oder Betriebsdatensätze; Workflow-Engines, automatisierte Entscheidungsregeln und Eskalationsregeln; Anwendungsprogrammierschnittstellen sowie Interoperabilitäts- und Datenaustauschmechanismen; Mechanismen für Identität, Authentifizierung, Autorisierung, Berechtigungsnachweise und Zugangskontrolle; Protokollierungs-, Überwachungs-, Ranking-, Filter-, Abgleichs-, Empfehlungs- und Benachrichtigungssysteme; Plattformarchitektur, Cloud-Konfigurationen und eingebettete Sicherheitskontrollen; technische Spezifikationen, Beschaffungsanforderungen, Lizenzbedingungen und vom Lieferanten kontrollierte Systemfunktionen; sowie Protokolle der Mensch-Maschine-Interaktion, soweit diese Protokolle die Ausübung öffentlicher Gewalt strukturieren, begrenzen, kanalisieren oder lenken.

I.3.3 Recht, politische Vorgaben, Verwaltungsvorschriften, Verträge und menschliches Ermessen sind nicht schon deshalb selbst Code, weil sie niedergeschrieben oder formalisiert sind. Sie fallen nur insoweit unter die Begriffsbestimmung, als sie in ein digitales System übersetzt, in ein solches eingebettet oder durch ein solches operativ wirksam gemacht werden.

I.3.4 Hoheit über den Code bezeichnet die rechtlich begründete und institutionell wirksame Fähigkeit der Behörden, die technischen Systeme, durch die öffentliche Aufgaben wahrgenommen werden, zu verstehen, zu lenken, zu begrenzen, zu prüfen, zu testen, zu beanstanden, zu korrigieren, zu übersteuern, auszusetzen, zu ersetzen und erforderlichenfalls zu beenden. Sie setzt voraus, dass die verantwortliche Institution Folgendes bewahrt: die rechtliche Verantwortung für die Aufgabe; ausreichendes institutionelles Wissen und ausreichende technische Sachkunde; den Zugang zu den einschlägigen Nachweisen, Aufzeichnungen, Daten, Modellen, Konfigurationen, Protokollen und Auditinformationen; die wirksame Kontrolle über wesentliche Änderungen des Systems; die Fähigkeit, für Benachrichtigung, Erläuterung, Überprüfung, Anfechtung, Korrektur und Rechtsbehelfe zu sorgen; die operative Kontinuität, wenn ein Lieferant, eine Plattform, ein Modell oder eine Infrastrukturkomponente ausfällt oder nicht mehr verfügbar ist; sowie die Befugnis und die praktische Fähigkeit einzugreifen, wenn das System rechtswidrige, verfassungsrechtlich fehlerhafte, unsichere, diskriminierende, unzuverlässige oder institutionell nicht hinnehmbare Ergebnisse hervorbringt.

I.3.5 Hoheit über den Code setzt nicht voraus, dass eine öffentliche Institution Eigentümerin ihrer Software ist oder diese unmittelbar selbst entwickelt. Auslagerung, Beschaffung, Lizenzierung, Cloud-Abhängigkeit, proprietäre Systeme und die Beteiligung der Privatwirtschaft sind mit der Hoheit über den Code vereinbar, sofern sie der verantwortlichen Institution nicht die praktische Fähigkeit nehmen, ihre Rechtspflichten zu erfüllen.

I.3.6 Folgenabschätzung im digitalen öffentlichen Recht (DPLIA) ist die in Teil II geregelte maßgebliche Methode des Standards, um die öffentlich-rechtlichen Folgen einer digital vermittelten öffentlichen Aufgabe zu ermitteln, zu analysieren, über sie zu entscheiden, sie zu dokumentieren und zu überprüfen. Die DPLIA ist Teil des Standards und kein eigenständiges Instrument.

I.3.7 Akte der digitalen öffentlichen Aufgabe („die Akte“) ist die einzige maßgebliche Unterlage, in der eine Bewertung nach dem Standard dokumentiert wird (III.2).

I.3.8 Verantwortliche Institution ist die öffentliche Institution, die für die zu bewertende öffentliche Aufgabe rechtlich verantwortlich ist.

ENTWURF

I.3.9 Zuständige Behörde ist eine öffentliche Stelle, die rechtlich befugt ist, dem Standard in ihrem Zuständigkeitsbereich Wirkung zu verleihen; **Annahmeinstrument** ist das Instrument, durch das sie dies tut (III.5).

I.3.10 Feststellungsbericht am Maßstab des Standards ist das Ergebnis einer Bewertung auf jeder Prüfstufe (III.4). Er ist kein Zertifikat, kein Konformitätszeichen und keine Erklärung der Rechtmäßigkeit.

I.4 Die Kernanforderung

> **Kernanforderung**
>
> Jede Institution, die für eine digital vermittelte öffentliche Aufgabe rechtlich verantwortlich ist, muss die Befugnis, das Wissen, den Zugang, die Nachweise, die Kapazitäten und die praktischen Mittel bewahren, die erforderlich sind, um die technischen und soziotechnischen Arrangements, durch die diese Aufgabe wahrgenommen wird, zu verstehen, zu lenken, zu begrenzen, zu prüfen, zu beanstanden, zu korrigieren, zu übersteuern, auszusetzen, zu ersetzen und erforderlichenfalls zu beenden.

I.4.1 Ob die Kernanforderung erfüllt ist, wird anhand der zehn bewahrten Fähigkeiten (I.6) und der sechs Kontrollpunkte (II.3) geprüft. Eigentumsklauseln und Grundsatzerklärungen sind von Belang, aber kein Nachweis. Maßgeblich ist in jedem Fall, ob Rechte, Zugang, Befugnisse, Nachweise und operative Kapazitäten vorhanden, zugewiesen und nutzbar sind und unter realistischen Bedingungen erprobt wurden.

I.5 Grundsätze

Die folgenden elf Grundsätze legen die Mindestbedingungen dafür fest, dass öffentliche Aufgaben rechtmäßig, in verfassungsrechtlicher Kontinuität, institutionell verantwortet und resilient digital vermittelt werden.

Grundsatz 1. Bestimmung der öffentlichen Aufgabe. Jede digital vermittelte Tätigkeit muss nach ihrer Funktion und ihren tatsächlichen Wirkungen bewertet werden, nicht nach ihrer institutionellen Bezeichnung, ihrer Vertragsform, ihrem Eigentumsmodell oder ihrer technologischen Beschreibung.

Grundsatz 2. Rechtsgrundlage und verfassungsrechtliche Kontinuität. Die digitale Transformation darf die fortdauernde Geltung von Gesetzmäßigkeit, Zuständigkeit, Verfahrensfairness, Gleichheit, Verhältnismäßigkeit, Begründungspflicht, Rechenschaftspflicht, gerichtlichem Rechtsschutz und wirksamem Rechtsbehelf nicht unterbrechen.

Grundsatz 3. Nicht delegierbare öffentliche Verantwortung. Die verantwortliche öffentliche Institution muss die rechtliche und institutionelle Verantwortung für die öffentliche Aufgabe behalten, auch wenn technische Entwicklung, Betrieb, Infrastruktur, Datenverarbeitung oder Entscheidungsunterstützung von einem privaten Akteur erbracht werden.

Grundsatz 4. Institutionelle Hoheit über den Code. Die verantwortliche Institution muss in ausreichendem Maß rechtliche Befugnisse, technischen Zugang, Wissen, vertragliche Rechte, organisatorische Kapazitäten und operative Fähigkeiten bewahren, um das betreffende System zu verstehen, zu

beaufsichtigen, zu testen, zu korrigieren, zu übersteuern, auszusetzen, zu ersetzen oder zu beenden. Die Nachweise dafür werden nach den vier Nachweisbereichen (I.7) geordnet.

Grundsatz 5. Rückverfolgbarkeit und Integrität der Nachweise. Das System muss hinreichende Nachweise über seine Rechtsgrundlage, seine Gestaltungsannahmen, Datenquellen, Betriebsregeln, wesentlichen Änderungen, Entscheidungen, Eingriffe, Fehler und Ergebnisse erzeugen und sichern.

Grundsatz 6. Anfechtbarkeit und Rechtsbehelf. Betroffenen Personen müssen Benachrichtigung, Erläuterung, Überprüfung, Korrektur, Anfechtung und Rechtsbehelf in substanzieller Form offenstehen, die der Art und den Folgen der digital vermittelten öffentlichen Aufgabe angemessen ist.

Grundsatz 7. Governance über alle sechs Schichten hinweg. Die Einhaltung des anwendbaren Rechts kann nicht allein dadurch festgestellt werden, dass der Algorithmus oder die technische Komponente geprüft wird. Die rechtliche, die institutionelle, die technische, die datenbezogene, die operative und die gesellschaftliche Schicht sind gemeinsam zu bewerten.

Grundsatz 8. Kontrolle über private Akteure und Abhängigkeiten. Verträge, Lizenzen, Beschaffungsvereinbarungen, Beschränkungen aus Rechten des geistigen Eigentums, Cloud-Abhängigkeiten, Plattformregeln und proprietäre Systeme dürfen die Behörde nicht daran hindern, ihre Rechtspflichten zu erfüllen oder wirksame Kontrolle auszuüben.

Grundsatz 9. Sicherheit, Resilienz und Kontinuität. Das digitale System muss so gestaltet und gesteuert werden, dass die Kontinuität, Integrität, Verfügbarkeit und Wiederherstellbarkeit der öffentlichen Aufgabe sowie ihre rechtmäßige Wahrnehmung bei vorhersehbaren Störungen, Ausfällen, Angriffen, dem Rückzug eines Lieferanten oder technologischem Wandel gewahrt bleiben.

Grundsatz 10. Absicherung über den Lebenszyklus. Die Bewertung muss nach Beginn des Einsatzes fortgesetzt werden. Wesentliche Änderungen des Rechts, des Zwecks, der Daten, der Modelle, der Systemkonfiguration, der Lieferanten, der Infrastruktur, des Risikos oder der institutionellen Kapazitäten müssen eine verhältnismäßige Neubewertung auslösen.

Grundsatz 11. Institutionelle Gesamtwürdigung. Die abschließende Entscheidung darf nicht auf einen technischen Punktwert oder ein automatisiertes Konformitätsergebnis verkürzt werden. Die verantwortliche Institution muss eine begründete öffentlich-rechtliche Würdigung vornehmen und dokumentieren, die sich auf die sechs Kontrollpunkte, die Analyse der sechs Schichten, die kausale Synthese, die Belastbarkeit der Nachweise, die Restrisiken und die Auflagen für den weiteren Betrieb stützt.

I.6 Die zehn bewahrten Fähigkeiten

I.6.1 Die Kernanforderung erhält ihren operativen Gehalt durch zehn bewahrte Fähigkeiten. In kanonischer Reihenfolge sind dies: Verstehen → Lenken → Dokumentieren → Auditieren → Erläutern → Korrigieren → Eingreifen → Beweise sichern → Fortführen → Aussteigen.

I.6.2 Die Fähigkeiten gelten kumulativ, nicht wahlweise. Die Stärke einer Fähigkeit kann das Fehlen einer anderen Fähigkeit, die zur Erfüllung der mit der Aufgabe verbundenen Rechtspflichten notwendig ist, nicht ausgleichen, und alle zehn werden gemeinsam betrachtet.

ENTWURF

I.6.3 Das Eigentum am Quellcode ist nicht ausschlaggebend. Je nach der verfassungsrechtlichen Bedeutung der Aufgabe und der Art einer etwaigen Abhängigkeit von privaten Akteuren kann der Zugang zum Quellcode unerlässlich, hilfreich, aber nicht unerlässlich, oder entbehrlich sein. Die Frage ist eine funktionale, keine eigentumsrechtliche.

I.6.4 Wie weit jede Fähigkeit reichen muss, richtet sich nach der verfassungsrechtlichen Bedeutung der Aufgabe, der Schwere und Umkehrbarkeit möglicher Wirkungen, dem Grad der Abhängigkeit von privaten Akteuren und der Schwierigkeit, auf die eine betroffene Person stieße, wenn sie Nachweise über das Geschehene erlangen wollte. Der Standard begründet keine verschuldensunabhängige Haftung für jedes Systemversagen und verlangt nicht, dass jede Behörde eigene Fähigkeiten zur Softwareentwicklung vorhält.

Nr.	Fähigkeit	Erforderliches Können der Institution	Beispielhafte Nachweise	Nachweisbereich
1	Verstehen	Beschreiben, wie das Arrangement die Aufgabe wesentlich beeinflusst, wo seine operativen Grenzen liegen und welche Ausfallarten bekannt sind.	Aufgabenkarte; Architekturbeschreibung; Analyse der Grenzen; Nachweis der Sachkunde des Personals; unabhängige technische Erläuterung.	Kennen
2	Lenken	Die rechtmäßigen Zwecke, die maßgeblichen Richtlinien, die operativen Schwellenwerte, den betroffenen Personenkreis und jede wesentliche Änderung daran bestimmen.	Verzeichnis der Entscheidungsbefugnisse; Änderungsfreigabe; durchsetzbare Vertragsbestimmungen zur Änderungskontrolle beim Lieferanten; Freigabeprotokoll.	Steuern
3	Dokumentieren	Die einschlägigen Daten, Regeln, Versionen und Eingriffe sowie den Weg rekonstruieren, auf dem eine Entscheidung zustande kam.	Datenherkunft; Konfigurations- und Versionshistorie; administrative und technische Aufzeichnungen.	Kennen
4	Auditieren	Eine qualifizierte, angemessen unabhängige Prüfung von Leistung, Protokollen, Kontrollen und beim Lieferanten liegenden Nachweisen ermöglichen. Das Auditrecht ausüben, nicht nur innehaben.	Ausübbare Zugangsrechte; abgeschlossene Audits; Testergebnisse; Aufzeichnungen über den Zugang.	Verantworten
5	Erläutern	Verständliche, einzelfallbezogene Gründe angeben, die ausreichen, damit die betroffene Person eine Entscheidung verstehen und gegebenenfalls anfechten kann.	Erläuterungstests mit Nutzenden; begründete Entscheidungen; Begründungsvorlagen; Offenlegungsverfahren.	Kennen

Nr.	Fähigkeit	Erforderliches Können der Institution	Beispielhafte Nachweise	Nachweisbereich
6	Korrigieren	Fehler in Daten, Logik und Ergebnissen erkennen und korrigieren und die Korrektur auf jede Entscheidung übertragen, die von dem Fehler betroffen war.	Tests der Korrektur und ihrer Übertragung; Ermittlung der betroffenen Fälle; Aufzeichnungen über das Wiederaufgreifen.	Verantworten
7	Eingreifen	Den Betrieb durch befugtes Handeln übersteuern, einschränken, aussetzen oder sicher auf einen früheren Stand zurücksetzen.	Erprobte Eingriffsverfahren; geschulte Bedienstete; Eskalationsbefugnis und Eskalationsprotokolle.	Steuern
8	Beweise sichern	Beweise im Rahmen rechtmäßiger Aufbewahrungsregeln für Beschwerden, Überprüfung, Gerichtsverfahren, Untersuchungen und institutionelles Lernen nutzbar halten.	Aufbewahrungsplan; Löschsperre (Legal Hold); geschützte Protokolle; Zugangskontrollen.	Verantworten
9	Fortführen	Grundlegende Rechtspflichten auch bei einem Systemausfall, einem Angriff oder dem Ausfall eines Lieferanten erfüllen.	Erprobte Rückfallebene; alternativer Kanal; Wiederherstellungsübungen; Ressourcen für die Kontinuität.	Aufrechterhalten
10	Aussteigen	Ein System oder ein Lieferantenverhältnis migrieren, ersetzen oder beenden und dabei die zugrunde liegende Rechtspflicht weiter erfüllen.	Übergang mit Kostenschätzung; Übertragbarkeitstests; Unterstützungsrechte; Wahrung anhängiger Ansprüche; abgeschlossene Ausstiegsübung.	Aufrechterhalten

Tabelle I.1. Die zehn bewahrten Fähigkeiten in kanonischer Reihenfolge mit dem Nachweisbereich, dem jede von ihnen zugeordnet ist.

I.6.5 Die Aufzeichnungen müssen für Rekonstruktion und Abhilfe ausreichen und zugleich die rechtlichen Vorgaben zu Datenminimierung, Vertraulichkeit und Aufbewahrungsfristen wahren. Die Korrektur muss jede betroffene Entscheidung ermitteln und einen rechtmäßigen Weg zu ihrer Behandlung eröffnen, wobei etwaige Grenzen des Wiederaufgreifens und ihre Folgen zu dokumentieren sind.

I.7 Die vier Nachweisbereiche

I.7.1 Die vier Nachweisbereiche ordnen die zehn Fähigkeiten nach der Art der Nachweise, die jede von ihnen erfordert. Sie sind eine Ordnungshilfe für Nachweise, kein zweiter einzustufender Katalog, und sie ändern die kanonische Reihenfolge der Fähigkeiten nicht.

Nachweisbereich	Fähigkeiten	Frage	Typische Nachweise
Kennen	Verstehen · Dokumentieren · Erläutern	Kann die Institution beschreiben, wie die Aufgabe wahrgenommen wird, wo ihre Grenzen liegen und warum ein bestimmtes Ergebnis zustande kam?	Architektur, Datenherkunft, Abhängigkeitskarte, Nachweise zur Befähigung des Personals, Gründe im Einzelfall.
Steuern	Lenken · Eingreifen	Kann die Institution wesentliche Entscheidungen und Änderungen lenken und den Betrieb unterbrechen?	Vertrags- und Zugangsrechte, Aufzeichnungen zur Änderungskontrolle, ausgeübte (nicht bloß bestehende) Eingriffsrechte.
Verantworten	Auditieren · Korrigieren · Beweise sichern	Kann sich die Institution einer Prüfung stellen, Fehler korrigieren und Beweise für die Überprüfung sichern?	Abgeschlossene Audits, Aufzeichnungen über Korrekturen und ihre Übertragung, Aufzeichnungen über Aufbewahrung und Löschsperren.
Aufrechterhalten	Fortführen · Aussteigen	Kann die Institution ihre Rechtspflichten weiter erfüllen und aus einer Abhängigkeit aussteigen?	Übungsergebnisse, unabhängige Tests, Reaktion auf Vorfälle, Ausstiegsübungen.

Tabelle I.2. Die vier Nachweisbereiche.

I.8 Grundlegende Tests und Begriffe

I.8.1 Test des funktionalen Anwendungsbereichs

I.8.1.1 Der Standard gilt, wenn drei Voraussetzungen kumulativ erfüllt sind: (a) es wird öffentliche Gewalt ausgeübt – die Angelegenheit betrifft die Wahrnehmung, die Organisation, die Überprüfung oder die Kontinuität einer verfassungsrechtlich relevanten öffentlichen Aufgabe, unabhängig davon, ob diese unmittelbar von einer öffentlichen Stelle oder von einem in ihrem Auftrag handelnden privaten Akteur wahrgenommen wird; (b) ein digitales System beeinflusst diese Ausübung wesentlich und prägt ihren Inhalt, ihr Verfahren oder ihr Ergebnis so, dass diese ohne das System anders ausfielen; und (c) dieser Einfluss hat verfassungsrechtliche Bedeutung, weil er Gesetzmäßigkeit, Rechenschaftspflicht, Rechte, demokratische Governance oder institutionelle Resilienz berührt.

I.8.1.2 Wesentlicher Einfluss kann von Empfehlungen, Voreinstellungen, maßgeblichen Registern oder den kumulativen Wirkungen der Zuleitung zu Diensten ausgehen. Zu prüfen ist die tatsächliche Funktionsweise, nicht die Bezeichnung, die ein System trägt: Ein als Entscheidungsunterstützung beschriebenes Werkzeug kann Ergebnisse bestimmen, während Menschen nur nominell beteiligt sind.

I.8.1.3 Ist eine der Voraussetzungen nicht erfüllt, liegt die Angelegenheit außerhalb des Anwendungsbereichs des Standards. Alltägliche digitale Erleichterungen ohne wesentliche öffentlich-rechtliche Bedeutung liegen außerhalb des Anwendungsbereichs; gleichwohl kann auch ein kleines System erfasst sein, wenn es

Rechte oder die Überprüfung berührt. Ungewissheit beweist nicht, dass eine Aufgabe außerhalb des Anwendungsbereichs liegt: Eine ungewisse Abgrenzung erfordert Nachweise und eine dokumentierte vorläufige Bewertung, und die Abgrenzung wird erneut geprüft, wenn sich die Aufgabe oder ihre Abhängigkeiten wesentlich ändern.

I.8.2 Privatakteur-Test

I.8.2.1 Wirkt ein privater Akteur an einer Aufgabe mit, die den Test des funktionalen Anwendungsbereichs besteht, so fragt der Privatakteur-Test, ob diese Mitwirkung nicht delegierbare öffentliche Verantwortung und verstärkte Kontrollen auslöst. Seine Merkmale sind: (a) funktionale Substitution – der Akteur übernimmt eine Tätigkeit, die sonst die öffentliche Institution selbst ausführen müsste; (b) praktische Unverzichtbarkeit – beurteilt anhand von Dokumentation, Auditrechten, Kontrolle über Änderungen, Aufbewahrung der Nachweise und Ausstiegsfähigkeit; und (c) Verlagerung der Rechenschaftspflicht – die gewöhnliche öffentlich-rechtliche Rechenschaftspflicht (Begründung, Überprüfung, Rechtsbehelf) kann den Akteur nicht unmittelbar erfassen.

I.8.2.2 Sind alle Merkmale erfüllt, gilt für das Handeln des Akteurs derselbe strenge Maßstab wie für eine rein öffentliche Stelle, die dieselbe Aufgabe wahrnimmt, und es sind verstärkte Kontrollen erforderlich; eine schwerwiegende einzelne Abhängigkeit kann gezielte Schutzvorkehrungen rechtfertigen. Der Test ermittelt den Governance-Bedarf. Die Zurechnung zum Staat, die unmittelbare Haftung des Lieferanten und die Frage, ob der Akteur der gerichtlichen Überprüfung unterliegt, richten sich weiterhin nach dem anwendbaren Recht.

I.8.2.3 Der Test des funktionalen Anwendungsbereichs und der Privatakteur-Test beantworten nacheinander unterschiedliche Fragen und werden nicht zusammengeführt: Der erste bestimmt die öffentlich-rechtliche Angelegenheit; der zweite klärt, ob einen bestimmten privaten Beteiligten innerhalb dieser Angelegenheit öffentlich-rechtliche Pflichten treffen.

I.8.3 Sechsschichtige Governance-Architektur

Schicht	Kernfrage
1. Verfassungs- und rechtlich-regulatorische Schicht	Welche Befugnisse, Rechte, Pflichten und fachrechtlichen Vorschriften begründen die Aufgabe, und genügt der Auftrag der Gesetzmäßigkeit und der Verhältnismäßigkeit?
2. Institutionelle Verantwortung	Wer ist für die Aufgabe verantwortlich, wer finanziert, betreibt, beaufsichtigt und ändert sie, und lässt sich diese Verantwortung über Delegations- und Lieferantenbeziehungen hinweg zurückverfolgen?
3. Daten und Infrastruktur	Von welchen Registern, Modellen, Schnittstellen, Cloud-Diensten und Interoperabilitätsregelungen und von welcher Sicherheitsarchitektur hängt die Aufgabe ab?
4. Entscheidung und Leistungserbringung	Wie wird die Aufgabe dort wahrgenommen, wo entschieden wird – durch Algorithmen, Automatisierung oder eine Ermessensstruktur?
5. Rechenschaft und Aufsicht	Erreichen Begründung, Audit, Beschwerde, Rechtsmittel und gerichtliche Überprüfung die Aufzeichnungen, die auf der Entscheidungsschicht entstanden sind?

ENTWURF

Schicht	Kernfrage
6. Resilienz und Kontinuität	Was geschieht mit der Aufgabe bei einem Ausfall, beim Rückzug eines Lieferanten, bei einem Angriff, in einer Krise oder bei einem Übergang?

Tabelle I.3. Die sechsschichtige Governance-Architektur.

I.8.3.1 Die Schichten sind analytisch getrennt, institutionell aber voneinander abhängig. Ein Mangel auf einer Schicht tritt typischerweise auf einer anderen zutage: Eine nicht rückverfolgbare Verantwortung (Schicht 2) zeigt sich, wenn die Rechenschaftspflicht auf die Probe gestellt wird (Schicht 5); eine ungeprüfte Abhängigkeit (Schicht 3) wird bei der Vertragsverlängerung zur Kontinuitätskrise (Schicht 6). Die Architektur ist eine Karte der Kausalzusammenhänge, kein siebter Kontrollpunkt und keine parallele Checkliste.

I.8.4 Verfassungsinfrastruktur

I.8.4.1 Verfassungsinfrastruktur bezeichnet digitale Systeme – Identitätssysteme, Register, Cloud-Lösungen, Interoperabilitätsschichten –, die Teil der institutionellen Grundlagen geworden sind, auf denen Personen ihre Rechte ausüben und öffentliche Stellen verfassungsrechtliche Aufgaben wahrnehmen, sodass ihr Ausfall das Verfassungsleben unterbricht und nicht bloß betriebliche Unannehmlichkeiten verursacht. Eine Infrastruktur ist verfassungskritisch, wenn ihr Ausfall oder der Verlust der Kontrolle über sie die Ausübung grundlegender Rechte oder das rechtmäßige Handeln des Staates unmöglich machen würde.

I.8.5 Nicht delegierbare öffentliche Verantwortung

I.8.5.1 Eine Behörde kann eine Tätigkeit delegieren, ohne die mit ihr verbundene Verantwortlichkeit zu delegieren: Die Verantwortlichkeit kann nicht zusammen mit der Tätigkeit abgegeben werden. Die technische Auslagerung kann eine betroffene Person nicht ohne eine ihr gegenüber verantwortliche Institution oder ohne einen nutzbaren Weg zur Korrektur zurücklassen. „Der Lieferant ist verantwortlich“ ist kein rechtmäßiger Ersatz für die institutionelle Verantwortlichkeit.

ENTWURF

Teil II – Methode: Folgenabschätzung im digitalen öffentlichen Recht

II.1 Charakter der Methode

II.1.1 Der Standard legt fest, was erfüllt bleiben muss; die DPLIA ist die maßgebliche Methode des Standards, mit der geprüft wird, ob es bei einer bestimmten öffentlichen Aufgabe erfüllt ist. Die DPLIA ersetzt keine rechtlichen, technischen, risikobezogenen oder auf Rechte bezogenen Fachbewertungen, soweit diese weiterhin rechtlich vorgeschrieben sind. Sie würdigt deren Ergebnisse zusammen als Nachweise am Maßstab des Normativen Kerns.

II.1.2 Die Methode muss zu einem günstigen Ergebnis führen können, wenn die Nachweise es tragen. Ihr Wert liegt in der Qualität der Begründungen, Entscheidungen und Schutzvorkehrungen, nicht in der Zahl nachteiliger Feststellungen oder im Umfang der erstellten Dokumentation.

II.1.3 Kontrollpunkte führen zu Feststellungen, nicht zu Punktwerten. Ein Gesamtpunktwert wird nicht gebildet, und die Rechtmäßigkeit kann nicht dadurch festgestellt werden, dass günstige Einstufungen der Fähigkeiten addiert werden oder eine rechtswidrige Gestaltung gegen die erwartete Effizienz abgewogen wird.

II.2 Die sechs Schritte

II.2.1 Die DPLIA wird in sechs Schritten durchgeführt. Die Nummerierung der Schritte ordnet die Arbeit; sie erlaubt es nicht, für einen Kontrollpunkt abschließend die Feststellung „Erfüllt“ zu treffen, bevor die Nachweise geprüft sind, von denen er abhängt. Nachweise aus einem späteren Schritt können jede frühere Feststellung ändern, und eine wesentliche Änderung kann die Bewertung zu Schritt 1 zurückführen. Frühe Feststellungen sind vorläufig, soweit sie von später gewonnenen Nachweisen abhängen; die Institutionelle Entscheidung setzt voraus, dass sie miteinander in Einklang gebracht sind.

Schritt	Bezeichnung	Tätigkeit	Ergebnis in der Akte
1	Anwendungsbereich	Akte bei politischer Konzeption, Beschaffung, Vertragsverlängerung, wesentlicher Änderung oder einem Vorfall anlegen; verantwortliche Person, angestrebtes Ergebnis und anstehende Entscheidung bestimmen; Test des funktionalen Anwendungsbereichs anwenden; Prüfstufe festlegen (III.3).	Ergebnis der Vorprüfung; verantwortliche Person; Abgrenzung; Prüfstufe; Auslöser für eine erneute Prüfung.
2	Aufgabenkarte	Abgrenzung und Abhängigkeiten der Aufgabe bestimmen; die sechs Schichten abbilden; Privatakteur-Test anwenden; betroffene Personen ermitteln; übernommene Fachnachweise verzeichnen.	Aufgabenkarte; Verzeichnis der Abhängigkeiten und Nachweise; Analyse der betroffenen Personen.

ENTWURF

Schritt	Bezeichnung	Tätigkeit	Ergebnis in der Akte
3	Sechs Kontrollpunkte	Aufgabe an jedem Kontrollpunkt prüfen und die zehn Fähigkeiten einstufen; zu jeder Feststellung Quelle und Belastbarkeit der Nachweise dokumentieren.	Feststellungen zu den Kontrollpunkten mit Teilfeststellungen; Einstufungen der Fähigkeiten.
4	Kausale Synthese	Feststellungen zu Kontrollpunkten, Fähigkeiten und Schichten zusammen als Kausalketten lesen; Risiko, Belastbarkeit der Nachweise und Integrität der Umsetzung getrennt angeben.	Kausale Synthese; Restrisiken; abweichende Auffassungen.
5	Institutionelle Entscheidung	Begründete Entscheidung in einer von acht Kategorien treffen, mit Auflagen, verantwortlichen Personen, Fristen und Folgen.	Unterzeichnete Entscheidung; Auflagenverzeichnis; Feststellungsbericht.
6	Überprüfung im Lebenszyklus	Betrieb, Benachrichtigung und Abhilfe überwachen; planmäßig oder bei wesentlicher Änderung neu bewerten; Übergang oder Ausstieg steuern.	Überprüfungskalender; Auslöserprotokoll; aktualisierte Feststellungen.

Tabelle II.1. Die sechs Schritte der DPLIA.

Schritt 1 – Anwendungsbereich

II.2.2 Die Bewertung beginnt, sobald eine Aufgabe konzipiert wird, für sie eine Beschaffung oder eine Vertragsverlängerung erfolgt, sie wesentlich geändert wird oder von einem Vorfall betroffen ist. Die verantwortliche Institution legt die Akte an, benennt die rechenschaftspflichtige Person und hält das für die Allgemeinheit angestrebte Ergebnis sowie die Entscheidung fest, die durch die Bewertung vorbereitet werden soll. Sie wendet den Test des funktionalen Anwendungsbereichs (I.8.1) einmal an, bevor ein Kontrollpunkt bewertet wird; der Test ist selbst kein Kontrollpunkt.

II.2.3 Für eine Aufgabe, die außerhalb des Anwendungsbereichs liegt, wird ein begründeter Vorprüfungsvermerk erstellt, der die verantwortliche Person und einen Auslöser für eine erneute Prüfung nennt. Die allgemeinen rechtlichen und administrativen Pflichten gelten weiter. Für eine Aufgabe innerhalb des Anwendungsbereichs bestimmt die Institution die Prüfstufe nach III.3 und hält die Gründe fest.

Schritt 2 – Aufgabenkarte

II.2.4 Die Aufgabenkarte bestimmt die Abgrenzung und die Abhängigkeiten der Aufgabe: die Akteure, Daten, Systeme, Lieferanten, Rechtsbehelfe und Rückfallebenen, auf die sie angewiesen ist. Sie bildet die Aufgabe über die sechs Schichten ab (I.8.3), wendet den Privatakteur-Test (I.8.2) auf jeden wesentlichen privaten Beteiligten an und ermittelt die betroffenen Personen, ihre Schutzbedürftigkeit und die berührten Interessen.

II.2.5 Fachnachweise – eine Datenschutz-Folgenabschätzung, eine Grundrechte-Folgenabschätzung, ein Sicherheitstest – werden durch Verweis verzeichnet, unter Angabe von Quelle, Version, verwahrender Stelle, rechtlichem Anwendungsbereich und Verifizierungsstatus. Ein abgeschlossener Fachbericht ist ein

Nachweis, der zu würdigen ist, keine maßgebliche Antwort auf jede Frage seines Fachgebiets. Entscheidend ist, was er für diese Aufgabe belegt und was an den Schnittstellen ungeklärt bleibt.

Schritt 3 – Die sechs Kontrollpunkte

II.2.6 Die sechs öffentlich-rechtlichen Kontrollpunkte („sechs Kontrollpunkte“) überführen die für die Aufgabe geltenden rechtlichen und verfassungsrechtlichen Anforderungen in ausdrückliche Feststellungen. Jeder Kontrollpunkt nennt eine Leitfrage, die von ihm erfassten Gegenstände und eine Sperrregel. Eine vollständige Bewertung behandelt alle sechs Kontrollpunkte; wird eine Teilfrage als nicht einschlägig behandelt, bedarf dies einer dokumentierten Begründung.

Kontrollpunkt	Leitfrage	Umfasst	Sperrregel
1. Rechtmäßiger Auftrag	Hat die Institution für diese Aufgabe eine spezifische rechtliche Zuständigkeit und verfolgt sie damit ein legitimes öffentliches Ziel?	Sachliche und örtliche Zuständigkeit; Bestimmtheit der Rechtsgrundlage; öffentlicher Zweck und betroffener Personenkreis; Zweckbindung; Übereinstimmung zwischen der im Code umgesetzten Regel und der Rechtsvorschrift.	Mit der Aufgabe darf nicht fortgefahren werden, ohne dass für ihren Zweck und ihren Personenkreis eine benennbare, geltende und hinreichend bestimmte Rechtsgrundlage besteht.
2. Grundrechtlich gerechtfertigte Gestaltung	Ist die Gestaltung angesichts der verfügbaren Alternativen erforderlich, verhältnismäßig, diskriminierungsfrei und zugänglich?	Nachweise zum Problem sowie Alternativen; mildere Mittel; Nutzen, Belastungen und Umkehrbarkeit; Auswirkungen auf Gruppen und Verteilungswirkungen; Zugänglichkeit; Schutzbedürftigkeit.	Mit einer Gestaltung darf nicht fortgefahren werden, wenn ein milderes Mittel dasselbe Ziel erreicht oder wenn bei einer Aufgabe der Prüfstufe 2 oder 3 die Auswirkungen auf Gruppen nicht bewertet sind. Berichterstattung kann eine rechtswidrige Diskriminierung oder einen unverhältnismäßigen Eingriff nicht heilen.
3. Öffentliche Verantwortung	Ist eine einzelne öffentliche Institution mit einem namentlich benannten Entscheidungs-verantwortlichen bestimmbar und für die Aufgabe verantwortlich?	Rechtmäßige Zuweisung der Verantwortung an öffentliche, private und verteilte Akteure; Regelungen zu Delegation, Beschaffung und Datennutzung; Eskalationswege.	Für die Aufgabe muss ein namentlich benannter Entscheidungsverantwortlicher der öffentlichen Hand feststehen, bevor eine Beschaffungsverpflichtung eingegangen wird.

Kontrollpunkt	Leitfrage	Umfasst	Sperrregel
4. Operative Kontrolle	Kann die Institution die Daten, den Code, die Lieferanten, die Änderungen und die Eingriffe, die die Aufgabe wesentlich prägen, rechtmäßig und wirksam steuern?	Rechtmäßiger Zugang zu Daten und rechtmäßige Datenkorrektur; vertragliche Kontrolle über wesentliche Abhängigkeiten; Änderungskontrolle, Versionierung, Zugang zu Protokollen und unabhängige Tests; Fähigkeit, zu auditieren, zu korrigieren, einzuschränken und umzulenken.	Kann die Institution bei einer Aufgabe mit erheblicher Wirkung auf Rechte eine wesentliche Auswirkung nicht auditieren, nicht in sie eingreifen oder sie nicht korrigieren, muss der Einsatz gesperrt werden, bis die Kontrolle nachgewiesen ist. Eine vertragliche Zusage, von der nie Gebrauch gemacht wurde, genügt für sich allein nicht.
5. Nachweise, Überprüfung und Rechtsbehelf	Können die Institution und eine betroffene Person ein erhebliches Ergebnis oder Versagen rekonstruieren, verstehen, anfechten und korrigieren?	Administrative und technische Nachweise; verständliche Begründung; substanzielle menschliche oder institutionelle Überprüfung; Vorbereitung auf Beschwerde, Rechtsmittel, Ombudsstelle, Regulierungsbehörde und gerichtliche Überprüfung; Korrektur individueller und systemischer Fehler einschließlich der Übertragung der Korrektur.	Fehlen bei einer Aufgabe mit erheblicher Wirkung auf Rechte ausreichende Nachweise, eine substanzielle Anfechtungsmöglichkeit oder eine wirksame Korrektur, muss der reguläre Einsatz gesperrt werden. Eine veröffentlichte Beschreibung oder eine nur nominelle menschliche Präsenz begründet keinen Rechtsbehelf.
6. Kontinuität und Ausstieg	Kann die Institution ihre Rechtspflichten bei Systemausfall, Angriff, Lieferantenausfall, Änderung, Vertragsverlängerung oder Beendigung weiter erfüllen und aussteigen, ohne Rechte, Beweise oder die Leistungserbringung aufzugeben?	Erprobte Kontinuität und nicht digitale Rückfallebene; Leitung der Vorfallsbewältigung und sicherer eingeschränkter Betrieb; Übertragbarkeit, Wechsel und Unterstützung beim Übergang; Sicherung von Beweisen, anhängigen Verfahren und Korrekturen über den Übergang hinweg.	Kontinuität und Ausstieg müssen erprobt sein, bevor eine Entscheidung über die Verlängerung oder die Kündigung des Vertrags unausweichlich wird, und nicht erst, nachdem die Abhängigkeit unumkehrbar geworden ist.

Tabelle II.2. Die sechs öffentlich-rechtlichen Kontrollpunkte

II.2.7 Kontrollpunkt 4 ist kein allgemeiner Punktwert für Cybersicherheit und entscheidet nicht darüber, ob einer betroffenen Person ein wirksamer Rechtsbehelf zur Verfügung steht; das ist die Frage von Kontrollpunkt 5. Kontrollpunkt 1 stellt die Rechtsgrundlage fest, die keine technische Fähigkeit verschaffen kann.

Schritt 4 – Kausale Synthese

II.2.8 Die Einhaltung des anwendbaren Rechts kann nicht dadurch festgestellt werden, dass der Algorithmus oder die technische Komponente isoliert geprüft wird. Die kausale Synthese liest die Feststellungen zu Kontrollpunkten, Fähigkeiten und Schichten zusammen als Ketten und fragt bei jeder wesentlichen Feststellung, (a) was die auslösende Bedingung ist; (b) über welche Schicht sie sich ausbreitet; (c) welche Schutzvorkehrung die Ausbreitung unterbrechen soll und ob diese Schutzvorkehrung tatsächlich angewandt oder lediglich dokumentiert worden ist; und (d) welches Restrisiko verbleibt, wenn die tatsächliche und nicht die bloß nominelle Wirkung der Schutzvorkehrung berücksichtigt wird. Eine günstige Bewertung jeder einzelnen Komponente kann diese Analyse ihres Zusammenwirkens nicht ersetzen.

II.2.9 Drei nachweisbezogene Würdigungen werden getrennt festgehalten und niemals zusammengeführt:

- **Risiko** – möglicher Schaden: Schwere, Wahrscheinlichkeit, Ausmaß, Dauer, Schutzbedürftigkeit, Umkehrbarkeit und Ausbreitung.
- **Belastbarkeit der Nachweise** – wie gut eine Feststellung gestützt ist: hoch, wenn aktuelle Nachweise verifiziert und angemessen erhärtet sind; mittel, wenn Zugang oder Tests eingeschränkt sind; gering, wenn Nachweise fehlen, unterstellt werden oder in wesentlichen Punkten bestritten sind.
- **Integrität der Umsetzung** – ob Schutzvorkehrungen in der Praxis zugewiesen, mit Mitteln ausgestattet, überwacht und durchsetzbar sind.

II.2.10 Eine als gering eingeschätzte Wahrscheinlichkeit kann fehlende Nachweise für die Rechtsgrundlage oder den Rechtsbehelf nicht heilen. Ein vertraglicher Anspruch belegt weder eine angemessene Personalausstattung noch eine wirksame Nutzung.

Schritt 5 – Institutionelle Entscheidung

II.2.11 Die verantwortliche Institution nimmt eine begründete öffentlich-rechtliche Würdigung in einer von acht Kategorien vor und dokumentiert sie.

Entscheidungskategorie	Anwendungsfall	Typischer Auslöser
Fortfahren	Für alle Kontrollpunkte lautet die Feststellung „Erfüllt“ oder „Nicht berührt“; die Fähigkeiten sind nachgewiesen, und die Belastbarkeit der Nachweise ist hoch.	Keine Fähigkeitslücke festgestellt.
Fortfahren unter durchsetzbaren Auflagen	Die Feststellungen zu den Kontrollpunkten lauten „Erfüllt“ oder „Bedingt erfüllt“; eine oder mehrere Schutzvorkehrungen weisen Schwächen auf, denen abgeholfen werden kann, mit namentlich benannter verantwortlicher Person und mit Frist.	Ein Auditrecht, das besteht, aber nicht erprobt ist.
Unter kontrollierten Bedingungen erproben	Eine neuartige Anwendung, zu der bislang nur prognostische Nachweise vorliegen.	Die Fähigkeit ist in der Gestaltung angelegt, hat sich im Betrieb aber noch nicht bewährt.

ENTWURF

Entscheidungskategorie	Anwendungsfall	Typischer Auslöser
Neu gestalten und erneut vorlegen	Für einen Kontrollpunkt lautet die Feststellung „Nicht erfüllt“, die Aufgabe bleibt nach einer Neugestaltung aber grundsätzlich rechtmäßig.	Keine Datenzugangs- oder Auditrechte gesichert.
Aussetzen	Das Versagen einer Fähigkeit gefährdet fortdauernd Rechte, während die Neugestaltung läuft.	Gegenwärtige Schadensgefahr.
Einstellen	Die Aufgabe kann in keiner umsetzbaren Gestaltung rechtmäßig wahrgenommen werden.	Nicht behebbare Nichterfüllung eines Kontrollpunkts.
Zusätzliche Rechtsgrundlage einholen	Die Aufgabe ist in ihrer Gestaltung tragfähig, ihr fehlt aber eine ausreichende Rechtsgrundlage.	Nichterfüllung von Kontrollpunkt 1 ohne Bezug zur operativen Kontrolle.
Zur unabhängigen Entscheidung vorlegen	Die Belastbarkeit der Nachweise ist zu gering, als dass die Bewertenden zu einem Ergebnis gelangen könnten.	Vom Lieferanten kontrollierte oder unzugängliche Nachweise.

Tabelle II.3. Die acht Kategorien der institutionellen Entscheidung.

II.2.12 Jede Entscheidung hält ihre Gründe, etwaige abweichende Auffassungen, die Schutzvorkehrungen, die Auflagen, die namentlich benannten verantwortlichen Personen, die Fristen und die Folge fest, die automatisch eintritt, wenn eine Auflage nicht fristgerecht erfüllt wird. Eine Auflage ohne verantwortliche Person und Frist ist keine Auflage. „Weiter überwachen“ oder „ist zu überwachen“ ist keine ausreichende Auflage.

II.2.13 Auflagen können Verbesserungen während des rechtmäßigen Betriebs regeln; Voraussetzungen müssen dagegen verifiziert sein, bevor die von ihnen abhängige Tätigkeit beginnt. Die Feststellung „Bedingt erfüllt“ erlaubt keinen regulären Einsatz in vollem Umfang, wenn eine sperrende Anforderung nicht erfüllt ist.

II.2.14 Ein Pilotbetrieb setzt eine bestehende Rechtsgrundlage, geschützte Teilnehmende, einen begrenzten Umfang und einen Abbruchmechanismus voraus. Er kann nicht als Ausnahme von einem Verbot oder als Ersatz für einen rechtlichen Auftrag dienen.

II.2.15 Die rechenschaftspflichtige Institution unterzeichnet die Entscheidung, bestimmt, wer die Erfüllung der Auflagen verifiziert, und hält die nächste Überprüfung fest. Die Abzeichnung durch den Lieferanten kann die öffentliche Entscheidung nicht ersetzen. Nachweise für einen gegenwärtigen Schaden erfordern unverzügliche rechtmäßige Schutzmaßnahmen, auch solange eine umfassendere Bewertung noch nicht abgeschlossen ist.

Schritt 6 – Überprüfung im Lebenszyklus

II.2.16 Die Bewertung endet nicht mit der Genehmigung oder dem Beginn des Einsatzes. Wesentliche Änderungen des Rechts, des Zwecks, der Daten, der Modelle, der Systemkonfiguration, der Lieferanten, der Infrastruktur, des Risikos oder der institutionellen Kapazitäten führen dazu, dass die betroffenen Kontrollpunkte erneut geprüft werden. Eine als Pilotbetrieb freigegebene Aufgabe darf ihren Personenkreis, ihren Zweck, ihre Daten oder ihre institutionelle Reichweite nicht ohne dokumentierte

Neubewertung ausweiten: Eine stillschweigende Ausweitung gibt es nicht. Eine Entscheidung gilt nur innerhalb des bewerteten Anwendungsbereichs und im Rahmen ihrer Auflagen; nicht erfüllte Auflagen führen zu der in der Entscheidung festgelegten Folge, einschließlich Einschränkung oder Aussetzung, soweit dies geboten ist.

II.2.17 Bei jeder Überprüfung bestätigt die Institution, dass

- ein Kalender der Neubewertungen und ein Auslöserprotokoll geführt werden und aktuell sind;
- jede Feststellung „Bedingt erfüllt" mit einer verantwortlichen Person, einer Frist, einer Verifizierungsmethode und einer Folge versehen ist;
- Kontinuität und Ausstieg erprobt worden sind, bevor eine Entscheidung über die Verlängerung oder die Kündigung des Vertrags unausweichlich wird;
- die Überprüfung nach Beginn des Einsatzes Vorfälle, Drift, Beschwerden, Korrekturen und ungleiche Auswirkungen untersucht hat.

II.2.18 Die Planung des Ausstiegs beginnt bei Gestaltung und Beschaffung, auch wenn seine Durchführung in Schritt 6 festgehalten wird. Bei Übergang oder Beendigung bleiben Leistungspflichten, Beweise, anhängige Ansprüche und die Rechenschaftspflicht gewahrt.

II.3 Feststellungen zu den Kontrollpunkten und Einstufung der Fähigkeiten

II.3.1 Feststellungen zu den Kontrollpunkten. Für jeden Kontrollpunkt wird genau eine begründete Feststellung getroffen:

Feststellung	Bedeutung
Erfüllt	Ausreichende Rechtsgrundlage und ausreichende Schutzvorkehrungen sind nachgewiesen.
Bedingt erfüllt	Die Anforderung kann durch eine durchsetzbare, fristgebundene Auflage vor oder während eines kontrollierten Einsatzes erfüllt werden. Die Auflage hat eine verantwortliche Person, eine Frist, eine Verifizierungsmethode und eine Folge für den Fall der Nichterfüllung.
Nicht erfüllt	Mit dem Arrangement kann ohne Neugestaltung, zusätzliche Rechtsgrundlage oder Einstellung nicht rechtmäßig fortgefahren werden.
Nicht feststellbar	Die Belastbarkeit der Nachweise ist für eine verantwortbare Schlussfolgerung zu gering; weitere Nachweise oder eine unabhängige Entscheidung sind erforderlich.
Nicht berührt	Die Aufgabe in ihrer festgelegten Abgrenzung berührt den Kontrollpunkt aus dokumentierten Gründen nicht.

Tabelle II.4. Die fünf Feststellungen zu den Kontrollpunkten.

II.3.2 Zu jeder Feststellung wird festgehalten, ob sie auf unmittelbaren, aus einer Fachbewertung übernommenen oder abgeleiteten Nachweisen beruht. „Teilweise" ist keine Feststellung zu einem Kontrollpunkt.

II.3.3 Fehlt eine ausreichende Rechtsgrundlage, eine rechenschaftspflichtige Institution, ein für die Überprüfung wesentlicher Nachweis oder ein substanzieller Rechtsbehelf, so sperrt dies den regulären

Einsatz mit erheblicher Wirkung auf Rechte. Eine verbotene oder rechtswidrig diskriminierende Verwendung kann nicht im Wege der Abwägung überwunden werden. Lautet die Feststellung zu einer nicht ausgleichbaren Anforderung „Nicht feststellbar“ und beruht dies auf fehlenden, nicht auf nachteiligen Nachweisen, so hat dies für den Einsatz dieselbe Folge wie die Feststellung „Nicht erfüllt“, bis ausreichende Nachweise vorliegen. Kritische Mängel der Kontinuität oder des Ausstiegs sperren ebenso ein Arrangement, dessen Ausfall die Erfüllung von Rechtspflichten unmöglich machen würde.

II.3.4 Einstufung der Fähigkeiten. Jede der zehn Fähigkeiten wird mit „Ja“, „Teilweise“ oder „Nein“ eingestuft. Die Bewertenden trennen bei jeder Fähigkeit drei Fragen, da eine positive Antwort auf die ersten beiden mit einer negativen Antwort auf die dritte vereinbar ist: (a) verfügt die Institution über die rechtliche Befugnis oder Berechtigung – einen gesetzlichen Auftrag, eine vertragliche Auditklausel, eine dokumentierte Befugnis zum Übersteuern; (b) verfügt sie über die praktischen Möglichkeiten und die Mittel, sie auszuüben – geschultes Personal, technischen Zugang, zeitliche Kapazität der Institution; und (c) ist die Fähigkeit unter realistischen Bedingungen nachgewiesen worden? Die Erprobung kann simuliert oder in gestellten Szenarien durchgeführt werden, wenn eine Erprobung im laufenden Betrieb Rechte oder die Kontinuität der Leistungserbringung gefährden würde.

II.3.5 Eine Angabe des Lieferanten ohne eigene Nachweise der Institution begrenzt die Einstufung auf „Teilweise“. Ein Vertrag, der Datenübertragbarkeit zusagt, belegt für sich allein nicht die Fähigkeit Aussteigen; eine Richtlinie, die menschliches Übersteuern erlaubt, belegt nicht die Fähigkeit Eingreifen, wenn den dazu ermächtigten Bediensteten die Zeit, die Informationen oder die Stellung fehlen, um davon Gebrauch zu machen; ein öffentliches Transparenzregister belegt nicht die Fähigkeit Erläutern in der Genauigkeit, die eine Anfechtung im Einzelfall erfordert; ein Auditrecht wird nur dann mit „Ja“ eingestuft, wenn es ausgeübt worden ist und nicht lediglich besteht.

II.3.6 Nachweisstufen. Nachweise für eine Schutzvorkehrung werden als „Dokumentiert“ (die Schutzvorkehrung besteht auf dem Papier), „Operativ“ (sie ist mindestens einmal angewandt worden) oder „Erprobt“ (sie ist unter realistischen Bedingungen erprobt worden) eingestuft. Welche Nachweisstufe mindestens erforderlich ist, richtet sich nach der Prüfstufe (III.3).

II.4 Orientierende Bezüge zwischen Fähigkeiten und Kontrollpunkten

II.4.1 Jede Bewertung legt dar, welche Einstufungen der Fähigkeiten die Feststellung zu jedem Kontrollpunkt stützen oder schwächen. Die nachstehenden Bezüge dienen der Orientierung und überschneiden sich; sie teilen die Fähigkeiten nicht in Gruppen ein und ersetzen die Nachweisbereiche nicht.

Kontrollpunkt	Fähigkeiten, die typischerweise Nachweise liefern
1. Rechtmäßiger Auftrag	Keine Fähigkeit kann eine Rechtsgrundlage verschaffen; Verstehen und Dokumentieren liefern Nachweise für die Übereinstimmung zwischen der im Code umgesetzten Regel und der Rechtsvorschrift.
2. Grundrechtlich gerechtfertigte Gestaltung	Verstehen, Lenken, Dokumentieren.
3. Öffentliche Verantwortung	Lenken, Dokumentieren.

ENTWURF

Kontrollpunkt	Fähigkeiten, die typischerweise Nachweise liefern
4. Operative Kontrolle	Lenken, Auditieren, Korrigieren, Eingreifen.
5. Nachweise, Überprüfung und Rechtsbehelf	Dokumentieren, Auditieren, Erläutern, Korrigieren, Beweise sichern.
6. Kontinuität und Ausstieg	Eingreifen, Beweise sichern, Fortführen, Aussteigen.

Tabelle II.5. Orientierende Nachweisbezüge.

II.5 Der Lebenszyklus des Systems

II.5.1 Die sechs Schritte der DPLIA sind von den sechs Phasen des Lebenszyklus des Systems zu unterscheiden, auf den die DPLIA angewandt wird: (1) strategische Konzeption; (2) Gestaltung und Beschaffung; (3) Entwicklung und Einsatz; (4) Governance im Betrieb; (5) Überprüfung und Anpassung; und (6) Beendigung oder Übergang. Die DPLIA kann in jeder Phase angewandt werden, vollständig oder in der Tiefe, die die Prüfstufe verlangt. Die Verwendungsarten nach III.1 entsprechen diesen Phasen.

ENTWURF

Teil III – Anwendung

III.1 Sechs Verwendungsarten

III.1.1 Der Standard und die DPLIA werden in sechs miteinander verbundenen Verwendungsarten angewendet. Die ersten vier sind gewöhnliche Verwendungen im Lebenszyklus; die beiden weiteren erstrecken den Standard auf außergewöhnliche Ereignisse und auf die systemische Analyse. In jeder Verwendungsart liefert der Normative Kern den Maßstab und die DPLIA die Methode, mit der Mängel, Unsicherheiten, kausale Wechselwirkungen, erforderliche Schutzvorkehrungen und institutionelle Folgen untersucht werden.

Verwendungsart	Was geprüft wird
1. Vorausschauende Bewertung	Vor Gestaltung, Beschaffung oder gesetzlicher Ermächtigung: ob eine geplante digital vermittelte Aufgabe überhaupt rechtmäßig eingerichtet werden kann.
2. Überprüfung von Gestaltung und Entwicklung	In der Gestaltungs- und Aufbauphase: ob die entstehende Architektur die Kontrollpunkte erfüllt, bevor Festlegungen nur noch schwer rückgängig zu machen sind.
3. Bewertung vor dem Einsatz	Vor Freigabe, Genehmigung oder Betriebsaufnahme: ob die Aufgabe so, wie sie tatsächlich eingerichtet wurde – nicht wie ursprünglich geplant –, dem Standard entspricht.
4. Überprüfung im Betrieb und im Lebenszyklus	Im gewöhnlichen Betrieb: ob die Aufgabe dem Standard weiterhin entspricht und ob eine wesentliche Änderung eine Neubewertung erfordert.
5. Überprüfung nach Vorfall, Versagen, Beschwerde, Rechtsstreit oder Kontroverse	Aus Anlass eines bestimmten Ereignisses: an welchem Kontrollpunkt oder auf welcher Schicht das Ereignis einen Mangel offenlegt und welche Korrektur es erfordert.
6. Systemische, vergleichende, gesetzgeberische oder institutionelle Überprüfung	Über mehrere Aufgaben, Rechtsordnungen oder einen Sektor hinweg: Muster, die bei der Bewertung einer einzelnen Aufgabe nicht sichtbar werden.

Tabelle III.1. Die sechs Verwendungsarten.

III.1.2 Jede Verwendung erfordert eine bestimmte Folge für die Entscheidung und eine fortlaufende Überprüfung. Die Bewertung eines geplanten Systems kann zu einer Neugestaltung oder zum Verzicht auf den Einsatz führen; die Bewertung einer bestehenden Aufgabe kann neben längerfristiger Abhilfe sofortige Schutzmaßnahmen erfordern. Erst die Überprüfung im Lebenszyklus (Schritt 6) macht jede Verwendungsart wirksam: Eine Überprüfung, die in der Akte nichts ändert, hat keine institutionelle Entscheidung hervorgebracht.

III.2 Die Akte der digitalen öffentlichen Aufgabe

III.2.1 Für jede Bewertung wird genau eine maßgebliche Akte der digitalen öffentlichen Aufgabe geführt. Die Akte ist das institutionelle Gedächtnis der Bewertung und das Rückgrat ihrer Nachweisführung, kein

fakultativer Anhang. Sie ist eine in sich geschlossene Entscheidungsakte, kein Dokumentenlager: Sie bindet Fachnachweise durch Verweis ein und gibt dabei Quelle, Version, verwahrende Stelle und Verifizierungsstatus an, statt die zugrunde liegenden Verträge, Datensätze oder Protokolle zu duplizieren. Sie ist eine amtliche Verwaltungsakte und wird dementsprechend aufbewahrt.

III.2.2 Die Akte gliedert sich in sechs Abschnitte:

Abschnitt der Akte	Wesentlicher Inhalt
1. Vorprüfung und Prüfstufe	Aufgabe, verantwortliche Person, Auslöser, Feststellungen zum Anwendungsbereich, Prüfstufe mit Begründung, Abgrenzung, Überprüfungstermin.
2. Aufgabe und Rechtsgrundlage	Auftrag, Zweck, Entscheidungsweg, Abhängigkeiten, maßgebliche Systembeschreibung; die verantwortliche Institution und der rechenschaftspflichtige Entscheidungsträger; Systeme, Lieferanten und private Akteure.
3. Governance und betroffene Personen	Karte der sechs Schichten; Privatakteur-Test; Zuweisung der Verantwortung; betroffene Personen, ihre Interessen und ihre Schutzbedürftigkeit; Beteiligung.
4. Kontrollpunkte und Synthese	Feststellungen und Teilfeststellungen zu den Kontrollpunkten mit Nachweisquelle; Risiko, Belastbarkeit der Nachweise und Integrität der Umsetzung; Alternativen; kausale Synthese; abweichende Auffassungen.
5. Fähigkeiten und Entscheidung	Einstufung der zehn Fähigkeiten mit Nachweisstufen; Schutzvorkehrungen; die Institutionelle Entscheidung; Auflagen, verantwortliche Personen, Fristen und Folgen; Regelungen zu Überwachung, Abhilfe, Kontinuität und Ausstieg.
6. Öffentliche Rechenschaft und Lebenszyklus	Feststellungsbericht; öffentliche Zusammenfassung; Stellungnahmen aus Konsultationen; Registereintrag; Wege der Benachrichtigung und der Anfechtung; Überprüfungstermine, Auslöser, Vorfälle, Änderungen und spätere Entscheidungen.

Tabelle III.2. Die sechs Abschnitte der Akte der digitalen öffentlichen Aufgabe.

III.2.3 Die Vergabeunterlagen sollen als Voraussetzung für den Zuschlag die Audit-, Nachweis-, Änderungskontroll- und Ausstiegsrechte verlangen, die an den Kontrollpunkten 3, 4 und 6 geprüft werden. Ein Recht, das erstmals nach der Vertragsunterzeichnung geltend gemacht wird, belegt eine Lücke in der Akte und heilt sie nicht.

III.3 Prüfstufen

III.3.1 Jede Bewertung wird auf einer von drei Prüfstufen durchgeführt. Die Prüfstufe bestimmt, wer bewertet, in welchem Umfang Nachweise erforderlich sind und wie unabhängig die Überprüfung sein muss. Ihre Festlegung ist eine Würdigung der Verhältnismäßigkeit, die in Schritt 1 vorgenommen und bei jeder wesentlichen Änderung der Aufgabe erneut geprüft wird; sie ersetzt nicht die materiellen Feststellungen, die an den Kontrollpunkten getroffen werden.

	Prüfstufe 1 – Selbstbewertung	Prüfstufe 2 – Überprüfte Bewertung	Prüfstufe 3 – Unabhängige Bewertung
Wer bewertet	Die verantwortliche Institution.	Die verantwortliche Institution, mit Abzeichnung durch eine namentlich benannte überprüfende Person, die von der bewerteten Aufgabe unabhängig ist.	Eine von der verantwortlichen Institution unabhängige Stelle.
Typische Aufgaben (zur Orientierung)	Begrenzte öffentlich-rechtliche Bedeutung; umkehrbare Unterstützung; keine Automatisierung mit erheblicher Wirkung auf Rechte.	Wesentliche Auswirkungen auf Rechte, Dienste oder das Vertrauen der Öffentlichkeit; mäßige Unumkehrbarkeit.	Hohe verfassungsrechtliche Bedeutung oder Unumkehrbarkeit; starke Abhängigkeit von privaten Akteuren; schutzbedürftige Gruppen in großer Zahl; sperrende Feststellungen oder bestrittene Nachweise.
Mindestinhalt der Akte	Knappe Akte; namentlich benannte verantwortliche Person; einschlägige Nachweise; verhältnismäßige Überwachung. Kontrollpunkte können auf der Grundlage minimaler Nachweise als „Erfüllt“ oder „Nicht berührt“ festgehalten werden, wenn die Gründe angegeben sind.	Vollständige Akte; vollständige Analyse aller sechs Kontrollpunkte; öffentliche Zusammenfassung; Fachanhänge, soweit die Aufgabe sie erfordert.	Vollständiges Nachweisverzeichnis; Einbindung betroffener Personen; Genehmigung durch die Leitungsebene.
Mindestnachweisstufe	Dokumentiert.	„Operativ“ für jede wesentliche Schutzvorkehrung.	„Erprobt“ für die Fähigkeiten, die für Rechtmäßigkeit, Rechtsbehelf, Kontinuität und Ausstieg zentral sind.
Ergebnis	Feststellungsbericht am Maßstab des Standards.	Feststellungsbericht am Maßstab des Standards.	Feststellungsbericht am Maßstab des Standards.

Tabelle III.3. Die drei Prüfstufen.

III.3.2 Wahl der Prüfstufe. Die Prüfstufe richtet sich nach den Auswirkungen der Aufgabe, der Schutzbedürftigkeit der betroffenen Personen, dem Ausmaß, der Umkehrbarkeit, der Abhängigkeit von privaten Akteuren, der Neuartigkeit und der Nachweisasymmetrie. Bezeichnungen wie Justiz, Identität oder Sozialleistungen bestimmen die Prüfstufe nicht allein: Die Aufgabe, ihre Folgen und ihre Abhängigkeiten müssen analysiert werden.

III.3.3 Verfassungskritische Aufgaben. Eine Aufgabe, bei der verfassungskritische Infrastruktur betrieben wird (I.8.4), wird auf Prüfstufe 3 bewertet; zusätzlich erfordert sie eine verstärkte Erprobung von Kontinuität und Ausstieg, Übungen zur Vorfallsbewältigung, eine regelmäßige unabhängige Überprüfung, die Eintragung in das öffentliche Register und die Verantwortung der Leitungsebene für die Kontinuität wesentlicher öffentlicher Pflichten.

III.3.4 Rahmenbedingungen der Prüfung. Bedingungen von Gebern sowie grenzüberschreitende, notfallbedingte, sicherheitsempfindliche oder sektorspezifische Umstände können zusätzliche Anforderungen begründen. Sie senken in keinem Fall die Prüfstufe und verringern auch nicht die Tiefe der materiellen Bewertung. Für dieselbe Aufgabe gilt kein geringerer öffentlich-rechtlicher Maßstab, weil eine Bewertung zu Finanzierungszwecken in Auftrag gegeben wird.

III.3.5 Außerhalb des Anwendungsbereichs. Einer Aufgabe, die den Test des funktionalen Anwendungsbereichs nicht besteht, wird keine Prüfstufe zugewiesen. Für sie wird der in II.2.3 beschriebene Vorprüfungsvermerk angelegt.

III.4 Feststellungsbericht

III.4.1 Auf jeder Prüfstufe ist das Ergebnis einer Bewertung ein Feststellungsbericht am Maßstab des Standards. Er nennt: die Aufgabe und die verantwortliche Institution; die Prüfstufe sowie Identität und Unabhängigkeit der bewertenden oder überprüfenden Person; den Umfang, die Kriterien und die Nachweise, auf die er sich stützt, sowie den Zeitpunkt, zu dem die Nachweise verifiziert wurden; die Feststellung zu jedem Kontrollpunkt; die Einstufung der zehn Fähigkeiten und die Nachweisstufen; die Belastbarkeit der Nachweise; die von der verantwortlichen Institution getroffene Institutionelle Entscheidung, sofern eine solche getroffen wurde; und den nächsten Überprüfungstermin.

III.4.2 Ein Feststellungsbericht ist kein Zertifikat, kein Konformitätszeichen, keine Erklärung der Rechtmäßigkeit und keine Erklärung, dass ein System konform ist. Seine Feststellungen stützen die Entscheidung der zuständigen Institution, ersetzen sie aber nicht. Der Abschluss einer Bewertung begründet in keinem Fall eine Vermutung der Rechtmäßigkeit. Ein Feststellungsbericht gilt nur für den Umfang, die Version und das Datum, die in ihm festgehalten sind; einen Bericht, der auf einer Bewertung beruht, die nie in einer aktuellen Akte festgehalten wurde, erkennt der Standard nicht an.

III.5 Formen der Annahme und Rechtswirkung

III.5.1 Eine zuständige Behörde kann dem Standard Wirkung verleihen: als gesetzliche Pflicht; als ministerielle Weisung oder Verwaltungsvorschrift; als Standard für öffentliche Dienste oder die Justizverwaltung; als Beschaffungsanforderung; als Methode einer Regulierungsbehörde; als Maßstab einer Ombudsstelle oder eines Audits; als Schutzvorkehrung eines Gebers; oder als freiwillige Leitlinie. Seine Rechtswirkung richtet sich nach dem Annahmeinstrument.

III.5.2 Ein Annahmeinstrument soll die annehmende Stelle und ihre Zuständigkeit, die angenommene Version des Standards, die erfassten Aufgaben und die internen Folgen einer Nichteinhaltung benennen. Es unterscheidet bestehende Rechtspflichten von zusätzlichen Verpflichtungen, die als institutionelle Leitlinie übernommen werden.

ENTWURF

III.5.3 Ein Annahmeinstrument soll mindestens vorsehen, dass

- jede geplante oder wesentlich geänderte digital vermittelte öffentliche Aufgabe einer Vorprüfung unterzogen wird, bevor beschafft, eingesetzt oder die Gestaltung unumkehrbar festgelegt wird;
- die verantwortliche Behörde benannt wird und die öffentlich-rechtliche Letztverantwortung nicht durch Vertrag übertragen darf;
- Aufgaben der Prüfstufe 3 und verfassungskritische Aufgaben einer unabhängigen Bewertung unterzogen werden;
- die Feststellungen zu den Kontrollpunkten von Risikopunktwerten und Nutzen getrennt gehalten werden;
- Fachbewertungen durch Verweis einbezogen und in einer einzigen übergreifenden Schlussfolgerung miteinander in Einklang gebracht werden;
- die Institution die zehn bewahrten Fähigkeiten in einem den Auswirkungen angemessenen Umfang vorhält;
- vorbehaltlich rechtmäßiger Ausnahmen öffentliche Zusammenfassungen bereitgestellt und Entscheidungen im Einzelfall begründet werden;
- Überwachung, Neubewertung, Reaktion auf Vorfälle und Ausstieg verbindliche Bestandteile des Lebenszyklus sind;
- die Akte der digitalen öffentlichen Aufgabe eine amtliche Verwaltungsakte ist und dementsprechend aufbewahrt wird.

III.5.4 Die Beschaffung soll die Regelungen zu Audit, Dokumentation, Änderungskontrolle, Eingriff, Kontinuität und Ausstieg sichern, die die Fähigkeiten erfordern. Kleinere Institutionen können gemeinsamen Sachverstand nutzen oder Rollen zusammenlegen, wenn Interessenkonflikte offengelegt werden und eine unabhängige Gegenprüfung gewahrt bleibt. Eine Institution soll dokumentieren, wie sie Personal, Überprüfung, Beteiligung und Erprobung finanzieren wird, statt Pflichten zu übernehmen, zu deren Erfüllung ihr die Kapazität fehlt.

III.5.5 Eine annehmende Institution soll ein öffentliches Register führen, das für jede bewertete Aufgabe die verantwortliche Institution, das Datum der Bewertung, die angewandte Version des Standards, die Prüfstufe, die Entscheidung, die nächste Überprüfung und einen zugänglichen Anfechtungsweg ausweist. Eine zweistufige Veröffentlichung kann sensibles Material schützen und zugleich die Rechenschaftspflicht stützen; jede Beschränkung der Offenlegung erfordert eine rechtmäßige, begründete Grundlage und einen angemessenen Zugang für zuständige unabhängige Überprüfungsstellen.

III.5.6 Die DPLIA soll in die bestehende Governance eingebunden und nicht einer abgesonderten Ethikstelle zugewiesen werden. Die Koordinierung kann bei einem Justizministerium, einer Regierungszentrale, einem staatlichen Digitaldienst, einer obersten Rechnungskontrollbehörde oder einer ressortübergreifenden Prüfstelle liegen; die operative Verantwortung verbleibt bei der Behörde, die die Aufgabe wahrnimmt.

ENTWURF

III.6 Beteiligung und Transparenz

III.6.1 Die Beteiligung beginnt, bevor wesentliche Entscheidungen feststehen. Die Akte hält fest, wer angehört wurde, wessen Erfahrungen noch fehlen, was sich daraufhin geändert hat und weshalb Alternativen verworfen wurden. Öffentliche Zusammenfassungen dienen der Auffindbarkeit; einzelfallbezogene Begründungen und nutzbare Beschwerdewege dienen dem Rechtsbehelf. Transparenz besteht auf drei Ebenen – Register, System und Einzelfall –, und ein Eintrag auf Registerebene erfüllt für sich allein weder die Anforderungen an die Begründung noch die an den Rechtsbehelf im Einzelfall.

III.7 Verhältnis zu anderen Instrumenten

III.7.1 Eine öffentliche Stelle kann jede fachrechtliche Pflicht für sich erfüllen, während die Aufgabe als Ganzes, die diese Pflichten gemeinsam berühren, unbewertet bleibt. Der Standard ist darauf angelegt, diese Lücke zu schließen, nicht darauf, mit den Instrumenten zu konkurrieren, die ihm Nachweise liefern. Neben diesen Instrumenten wird er wie folgt angewendet.

Instrument	Nachweise, die es liefert	Was der Standard hinzufügt
Rahmenübereinkommen des Europarats über künstliche Intelligenz und HUDERIA	Kontext, Beteiligung, Auswirkungen auf Menschenrechte, Demokratie und Rechtsstaatlichkeit sowie Minderungsmaßnahmen im gesamten Lebenszyklus der KI.	Die Ebene der verfassungsrechtlichen Rechtmäßigkeit und der institutionellen Kontrolle: rechtsordnungsspezifische Feststellungen zu den Kontrollpunkten, bewahrte Fähigkeiten und die institutionelle Entscheidung, über die Rechenschaft abzulegen ist, auch für Komponenten ohne KI.
Grundrechte-Folgenabschätzung nach der KI-Verordnung der EU (Art. 27)	Betroffene Personengruppen, spezifische Schadensrisiken, menschliche Aufsicht, interne Unternehmensführung und Beschwerdemechanismen innerhalb ihres rechtlichen Anwendungsbereichs.	Verantwortung und Abhängigkeiten über die gesamte öffentliche Aufgabe hinweg. Der Standard ersetzt die Grundrechte-Folgenabschätzung (FRIA) nicht.
Anforderungen der KI-Verordnung der EU an Hochrisiko-KI-Systeme	Nachweise zu den technischen und organisatorischen Anforderungen an das KI-System selbst.	Bewertung der öffentlichen Aufgabe als Ganzes statt des isoliert betrachteten Systems.
Datenschutz-Folgenabschätzung nach der DSGVO (Art. 35)	Zwecke der Verarbeitung, Notwendigkeit, Risiken, Garantien und Überprüfung.	Institutionelle Befugnis, Abhängigkeiten außerhalb der Verarbeitung, Rechtsbehelf insgesamt, Kontinuität und Ausstieg.
ISO/IEC 42001	Nachweise zur KI-Governance der Organisation.	Beide beantworten unterschiedliche Fragen. Eine Zertifizierung nach ISO/IEC 42001 ist ein relevanter Nachweis, aber kein Beweis der Rechtmäßigkeit.

Instrument	Nachweise, die es liefert	Was der Standard hinzufügt
Risikomanagement im Bereich der Cybersicherheit nach der NIS-2-Richtlinie	Resilienz von Netz- und Informationssystemen.	Rechtmäßigkeit, Rechte und Rechenschaftspflicht in Bezug auf die Aufgabe, der die Systeme dienen.
Interoperabilitätsbewertung nach der Verordnung für ein interoperables Europa	Rechtliche, organisatorische, semantische und technische Auswirkungen auf die grenzüberschreitende Interoperabilität.	Ob eine betroffene Person ein gleiches Recht ausüben kann, sobald Systeme Daten austauschen; Gesamtverantwortung und Kontinuität.
Kanadische Directive on Automated Decision-Making und AIA	Auswirkungsstufen, Konsultation des Rechtsdienstes, Tests, Überprüfung und Rechtsbehelfe.	Nachweise für die gesamte Aufgabe, wenn die digitale Vermittlung über den institutionellen oder systembezogenen Anwendungsbereich der Directive hinausreicht.
NIST AI RMF	Nachweise und Verfahren eines freiwilligen KI-Risikomanagements.	Die anwendbaren öffentlich-rechtlichen Pflichten und ihre Folgen für die institutionelle Entscheidung.

Tabelle III.4. Verhältnis zu anderen Instrumenten.

III.7.2 Die bestehenden Instrumente unterstützen eine solche Integration bereits: Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge kann eine einzige Datenschutz-Folgenabschätzung vorgenommen werden, und die KI-Verordnung sieht ausdrücklich vor, dass die Grundrechte-Folgenabschätzung eine Datenschutz-Folgenabschätzung ergänzt.

III.7.3 Der breite, auf Rechte und Rechtsstaatlichkeit gerichtete Ansatz von HUDERIA ist eine gehaltvolle Quelle anschlussfähiger Analyse; dass HUDERIA nicht verbindlich ist, mindert den Wert der Methodik nicht. Die kanadische AIA sieht bereits eine Überprüfung über den Lebenszyklus des Systems hinweg vor. Die DPLIA nutzt solche Arbeiten, statt die Lebenszyklusanalyse als ausschließlich eigenen Beitrag zu beanspruchen.

ENTWURF

Teil IV – Pflege des Standards und Umsetzung durch Soft Law

IV.1 Für die Pflege zuständige Stelle und Bezeichnung

IV.1.1 Der Standard wird vom Institute for Digital Society and Future Public Law („das Institut“) nach der Ordnung des Instituts gepflegt. Bis zu der in IV.1.2 beschriebenen Billigung wird er als „Standard des Instituts ‚Hoheit über den Code: Standard des digitalen öffentlichen Rechts‘“ bezeichnet, bis zu seiner Annahme mit dem Zusatz „Konsultationsentwurf“.

IV.1.2 Als EPLO-Standard oder Vorläufiger EPLO-Standard oder als von der EPLO gebilligt darf der Standard erst bezeichnet werden, nachdem der Exekutivausschuss der EPLO ihn nach der Ordnung über EPLO-Standards gebilligt hat. Die Billigung ändert den Wortlaut des Standards nicht.

IV.2 Konsultation, Annahme und Änderung

IV.2.1 Annahme und Änderung richten sich nach Artikel IV Absatz 3 Buchstabe f der Ordnung des Instituts, wonach der Wissenschaftliche Rat die Standards und Methodiken des Instituts auf Vorschlag des Direktors annimmt, und nach dem Beschluss des Wissenschaftlichen Rates über das Verfahren zur Ausarbeitung und Annahme von Standards des Instituts; daneben gilt die Ordnung über EPLO-Standards. Nach diesen Bestimmungen gilt:

- eine neue Version wird einer öffentlichen Konsultation von mindestens sechzig (60) Tagen unterzogen, jede andere inhaltliche Änderung einer öffentlichen Konsultation von mindestens dreißig (30) Tagen, und zu jeder Stellungnahme wird veröffentlicht, wie sie behandelt wurde;
- der Standard und jede seiner Änderungen werden vom Wissenschaftlichen Rat auf Vorschlag des Direktors angenommen, ohne Mitwirkung von Mitgliedern, die ein Interesse daran haben, einschließlich seiner Verfasser;
- jede angenommene Version trägt eine Versionsnummer und ein Datum und wird in ein vom Institut geführtes öffentliches Register eingetragen.

IV.2.2 Jede Änderung wird mit ihrer Begründung und einer Aufstellung der geänderten Anforderungen veröffentlicht. Sie gibt an, wie sie sich auf bereits abgeschlossene oder laufende Bewertungen auswirkt und welche Übergangsregelung gegebenenfalls gilt. Feststellungsberichte nennen die angewandte Version des Standards.

IV.2.3 Für die Pflege des Standards werden die Zuständigkeiten, die Beteiligungsverfahren, die Regeln zu Interessenkonflikten und die Versionshistorie veröffentlicht. An der Pflege werden öffentliche Institutionen, juristische und technische Fachleute, betroffene Gemeinschaften und unabhängige Forschende beteiligt.

IV.3 Soft-Law-Instrumente zur Umsetzung

IV.3.1 Der Standard wird durch Soft-Law-Instrumente umgesetzt: Leitgrundsätze; Musterklauseln und Mustervorschriften; Gutachten des Instituts; Aufforderungen zur Stellungnahme; Kommentare und

ENTWURF

Auslegungshinweise; Leitfäden für Schulung und Praxis; sowie Erklärungen zur Interoperabilität mit Instrumenten zwischenstaatlicher Organisationen.

IV.4 Bewertung, Audit und Validierung der Konformität

IV.4.1 Bewertung, Audit und Validierung der Konformität, die das Institut durchführt oder die für das Institut durchgeführt werden, beruhen auf einem vereinbarten Umfang, festgelegten Kriterien und überprüfbaren Nachweisen. Das Institut gibt seine Feststellungen als Feststellungsberichte am Maßstab des Standards heraus (III.4). Sie stützen die Entscheidung der zuständigen Institution, ersetzen sie aber nicht.

IV.4.2 Jede öffentliche Bestätigung von Ergebnissen, die das Institut von sich aus abgibt, bedarf eines gesonderten Beschlusses des Exekutivausschusses der EPLO.

IV.5 Rechtswirkung und öffentlicher Status

IV.5.1 Der Standard ist rechtlich nicht verbindlich, es sei denn, eine zuständige Behörde verleiht ihm durch ein eigenes Instrument Wirkung (III.5). Weder der Standard noch ein Feststellungsbericht verleiht rechtliche Befugnisse, begründet eine Vermutung der Rechtmäßigkeit oder verschafft dem Institut oder einer bewertenden Person einen vorbehaltenen öffentlichen Status.

IV.6 Personenzertifizierung

IV.6.1 Sobald eine Zertifizierungsstelle für die Kompetenz von Personen errichtet ist, wird die Zertifizierung hinter einer im Errichtungsbeschluss festgelegten Unparteilichkeits-Firewall zwischen Schulung, Bewertung und Zertifizierung erfolgen.

ENTWURF