Policy Brief:

Digitale Souveränität braucht überprüfbare Interoperabilität

Warum offene Standards alleine nicht ausreichen

Version 2
November 2026

4future.institute Policy Brief Series
Policy Brief Nr. 2026-002 (DE)
ISSN 3061-1881 (Online)
DOI: 10.5281/zenodo.24044216

Werner Illsinger
Executive Director
4future.institute
werneri@4future.institute

Dieser Policy Brief vertieft Abschnitt 3.2.2 des Policy Brief Nr. 2026-001 „Digitale Souveränität in Europa“ (Version 3, November 2026).
Er ersetzt die Version 1.1 vom Juni 2026.

Impressum

4future.institute · Graben 17/10 · 1010 Wien · Österreich · Telefon: +43 1 31440-0 · hello@4future.institute

4future.institute ist Teil der 4future.group und organisatorisch als unabhängige Einheit in der 4future business GmbH angesiedelt.

Firmenbuchnummer: FN 459359 d · Firmenbuchgericht: Handelsgericht Wien · UID-Nummer: ATU71656745 · Mehrheitseigentümerin: 4future.foundation

Über das 4future.institute: Zu fast jedem relevanten Thema unserer Zeit gibt es mehr Meinungen als Orientierung. Das 4future.institute fragt: Was stimmt hier eigentlich, was sind die strukturellen Bedingungen — und macht das Sinn, nicht nur wirtschaftlich, sondern für uns als Gesellschaft? Sein Orientierungsrahmen ist das 4future-Haus: Ziel ist ein gutes Leben für alle, heute und für kommende Generationen. Getragen wird es von drei Säulen, den drei V — Veränderung von Arbeit und Wirtschaft, Verteilungsgerechtigkeit und Versorgungssicherheit —, verbunden durch Rechtsstaat, bürgernahe Verwaltung und Koordination und gegründet auf europäische Grundwerte, Ethik und Nachhaltigkeit (Leitpapier „Strategie für eine lebenswerte Zukunft“, 4future.institute Papers Nr. 2026-001). Digitale Souveränität ist Teil der Versorgungssicherheit: digitale Dienste verlässlich nutzen, Anbieter wechseln und über eigene Daten entscheiden zu können. Die 4future.foundation ermöglicht die unabhängige Arbeit des Instituts; finanzielle Unterstützung begründet keinen Einfluss auf Inhalte oder Schlussfolgerungen.

Reihe: 4future.institute Policy Brief Series, Nr. 2026-002 (DE), ISSN 3061-1881 (Online), DOI: https://doi.org/10.5281/zenodo.24044216

Sprachfassungen: Englische Fassung: Policy Brief No. 2026-002 (EN). Bei Abweichungen ist die deutsche Fassung maßgeblich.

Versionen: Version 1.1 (Juni 2026); Version 2 (November 2026): in die Policy Brief Series aufgenommen, fachlich überarbeitet, Faktenstand und Quellen aktualisiert.

Offenlegung: Werner Illsinger ist Executive Director des 4future.institute, Geschäftsführer der 4future business GmbH und Vorstandsvorsitzender der 4future.foundation. Er hat zudem 4future.digital aufgebaut und ist dort als CTO tätig; 4future.digital bietet Cloud- und Kollaborationsdienste als europäische Alternative zu Microsoft 365 und Google Workspace an und setzt dabei die in diesem Papier behandelten offenen Standards ein. Von einer Interoperabilitätszertifizierung, wie sie dieses Papier vorschlägt, wäre 4future.digital als Marktteilnehmer betroffen. 4future.digital ist derzeit ein eigenständiges Unternehmen; Ziel ist, dass es wie die 4future business GmbH eine Tochter der 4future.foundation wird. Die 4future business GmbH erbringt selbst keine Cloud-Dienste. Empfehlungen des Instituts sind anbieterneutral formuliert; 4future.digital und seine Dienste werden im analytischen Teil dieses Papiers weder genannt noch bewertet.

Executive Summary

Digitale Souveränität zählt zu den zentralen strategischen Herausforderungen Europas. Die europäische Digitalpolitik reagiert darauf mit Investitionen in Infrastruktur, Cloud-Plattformen und regulatorischen Maßnahmen wie dem Digital Markets Act (DMA). Diese Initiativen sind notwendig – sie adressieren jedoch einen zentralen Aspekt digitaler Abhängigkeit bislang nur unzureichend:

die praktische Interoperabilität digitaler Systeme.

Offene Standards gelten seit Jahrzehnten als Grundlage digitaler Souveränität. Dieses Papier argumentiert jedoch, dass formale Offenheit allein nicht ausreicht. Entscheidend ist nicht nur die Existenz eines Standards, sondern dessen überprüfbare interoperable Umsetzung in der Praxis.

Die Realität digitaler Märkte zeigt eine zunehmende Differenz zwischen:

- formaler Standardisierung
  und
- tatsächlicher Austauschbarkeit.

Dokumentenformate, APIs, Kollaborationsplattformen und Kommunikationsprotokolle werden häufig formal unterstützt, praktisch jedoch asymmetrisch implementiert. Dominante Plattformökosysteme bieten typischerweise die vollständigste und risikoärmste Benutzererfahrung, während alternative Anbieter trotz Standardunterstützung strukturelle Interoperabilitätsnachteile tragen.

Dadurch entstehen:

- steigende Wechselkosten,
- langfristige Lock-in-Effekte
- und zunehmende Marktkonzentration.

Mit dem Übergang zu KI-gestützten Wissens- und Kollaborationssystemen verschärft sich diese Entwicklung zusätzlich. Die nächste Phase digitaler Abhängigkeit entsteht zunehmend auf Ebene:

- semantischer Wissensmodelle,
- Plattform-APIs,
- KI-Agenten
- und organisatorischer Kontextsysteme.

Das Papier schlägt daher eine europäische Interoperabilitätsstrategie vor. Kernpunkte sind:

- eine europäische Interoperabilitäts-Zertifizierung,
- standardisierte Compliance-Tests,
- offene Referenzimplementierungen
- sowie die stärkere Berücksichtigung interoperabler Standards in der öffentlichen Beschaffung.

Ziel ist nicht die Einschränkung technologischer Innovation, sondern die Schaffung offener und wettbewerbsfähiger digitaler Märkte.

Seit Version 1.1 hat sich der Rahmen bewegt: Die Europäische Kommission hat Zusagen Microsofts zu Teams für verbindlich erklärt, die Interoperabilität und Datenportabilität umfassen; sie hat vorläufig festgestellt, dass die Cloud-Dienste AWS und Microsoft Azure als Gatekeeper nach dem Digital Markets Act zu benennen sind; und mit den Vorschlägen für einen Cloud and AI Development Act (CADA) und für eine neue Vergabeverordnung liegen weitere Instrumente auf dem Tisch. Keines dieser Instrumente verlangt bislang, dass die praktische Interoperabilität und Wechselbarkeit von Büro- und Kollaborationsplattformen anhand offener, reproduzierbarer Tests nachgewiesen wird.

Die zentrale These dieses Papiers lautet:

Offene Standards allein reichen nicht aus.
Digitale Souveränität braucht überprüfbare Interoperabilität.

Inhaltsverzeichnis

1 Einleitung: Der blinde Fleck der digitalen Souveränität 9
1.1 Digitale Resilienz und geopolitische Handlungsfähigkeit 9
1.2 Digitale Souveränität als europäische Herausforderung 10
1.3 Infrastruktur allein reicht nicht 11
1.4 Standards als unsichtbare Machtstrukturen 11
1.5 Zielsetzung dieses Papiers 13
2 Standards als Grundlage digitaler Macht 14
2.1 Was Standards ermöglichen 14
2.2 Netzwerkeffekte und Plattformökonomie 14
2.3 Offene vs. proprietäre Standards 15
2.4 Open Source erzeugt nicht automatisch Wechselbarkeit 15
2.5 Formale Offenheit vs. praktische Interoperabilität 16
2.6 Standardisierung ohne überprüfbare Konformität 17
2.7 Der Unterschied zwischen Standardisierung und Austauschbarkeit 18
3 Der Kampf um Dokumentstandards 19
3.1 Die historische Dominanz proprietärer Office-Formate 19
3.2 Entstehung des OpenDocument Formats (ODF) 19
3.3 **Office Open XML (OOXML), ISO und das Strict/Transitional-Problem** 20
3.4 Warum Dokumentstandards über digitale Souveränität entscheiden 24
3.5 Langzeitarchivierung und staatliche Abhängigkeiten 25
4 Asymmetrische Interoperabilität in der Praxis 26
4.1 Wenn Standards nur „teilweise offen“ sind 26
4.2 E-Mail: IMAP als Second-Class Citizen 26
4.3 Kalender und Kontakte: in proprietären Ökosystemen 27
4.4 Proprietäre Erweiterungen, APIs und migrationsinduzierte Plattformbindung 30
4.5 „S3-kompatibel“ und andere Illusionen der Austauschbarkeit 32
5 Kollaborationsplattformen als neue Abhängigkeit 33
5.1 Vom Dokument zur Plattform 33

5.2 Teams, SharePoint und integrierte Arbeitsökosysteme 34
5.3 Workflow-Lock-in statt Dateiformat-Lock-in 35
5.4 Identität, Kommunikation und proprietäre Integration 36
5.5 Warum Wechselkosten mit jeder Integration wachsen 37
6 Der blinde Fleck des Digital Markets Act (DMA) 39
6.1 Ziele und Mechanismen des DMA 39
6.2 Gatekeeper-Regulierung und ihre Grenzen 39
6.3 Warum Arbeitsstandards kaum adressiert werden 41
6.4 Plattformmacht im Büro statt im App Store 41
6.5 Fehlende regulatorische Interoperabilitätsmechanismen 43
6.6 European Interoperability Framework und Interoperable Europe Act 44
6.7 Der Data Act: wichtiger Fortschritt – aber keine ausreichende Antwort auf moderne Plattformbindung 46
6.8 Der Cloud and AI Development Act (CADA) 48
7 Die nächste Lock-in-Welle: KI und semantische Plattformen 49
7.1 Von Dokumenten zu Wissensmodellen 50
7.2 Proprietäre KI-Ökosysteme 51
7.3 KI-Agenten und semantische Abhängigkeiten 52
7.4 APIs als neue Standards 53
7.5 Risiken für europäische digitale Souveränität 54
8 Warum offene Standards alleine nicht ausreichen 55
8.1 **Das Problem rein formaler Standardisierung** 55
8.2 **Fehlende Compliance-Prüfung** 55
8.3 **Fehlende Referenzimplementierungen** 56
8.4 **Fehlende Migrationsfähigkeit** 56
8.5 **„Open Washing" und Scheinkompatibilität** 56
8.6 Unterschiedliche Probleme, unterschiedliche Antworten 56
9 Vorschlag: Europäische Interoperabilitäts-Zertifizierung 58
9.1 Grundidee und Zielsetzung 58
9.2 Unabhängige europäische Zertifizierungsstelle 58

9.3 Technische Compliance-Tests ... 59
9.4 Referenzimplementierungen und Test-Suites ... 60
9.5 Zertifizierungsstufen, Durchsetzung und Finanzierung ... 62
9.6 Interoperabilität als Markttransparenz ... 65
9.7 Proportionalität, Offenheit und geringe Eintrittshürden ... 65
10 Öffentliche Beschaffung als strategischer Hebel ... 68
10.1 Die öffentliche Hand als Marktgestalter ... 68
10.2 Zertifizierung als Beschaffungsvoraussetzung ... 68
10.3 Förderung von Wettbewerb und Innovation ... 69
10.4 Chancen für europäische Anbieter ... 70
10.5 Langfristige Archivierung und Nachhaltigkeit ... 71
11 Handlungsempfehlungen ... 73
11.1 An die Europäische Kommission ... 74
11.2 An die österreichische Bundesregierung und EU-Mitgliedstaaten ... 75
11.3 An Normungs- und Standardisierungsorganisationen ... 76
11.4 An die Zivilgesellschaft und Wissenschaft ... 76
12 Schlussfolgerung ... 77
I. Über den Autor ... 80
II. Anhang: Begriffsbestimmungen ... 81
III. Anhang: Quellen & Literatur ... 89
Rechtsakte und Rechtsetzungsvorschläge der EU ... 89
Entscheidungen und Verfahren der Europäischen Kommission ... 89
Normen und Spezifikationen ... 89
Unternehmensdokumentation und Dokumentation zu Dokumentstandards ... 90
Marktdaten ... 90
Wissenschaftliche Literatur ... 91
Publikationen des 4future.institute ... 91

1 Einleitung: Der blinde Fleck der digitalen Souveränität

1.1 Digitale Resilienz und geopolitische Handlungsfähigkeit



Die zunehmende Konzentration kritischer digitaler Infrastruktur bei wenigen globalen Plattformanbietern erzeugt nicht nur wettbewerbliche, sondern auch geopolitische Risiken.

Europäische Unternehmen, Verwaltungen und öffentliche Institutionen sind heute in zentralen Bereichen von außereuropäischen Cloud-, Kommunikations- und Kollaborationsplattformen abhängig. Diese Abhängigkeit betrifft nicht nur Infrastruktur, sondern zunehmend auch organisatorische Arbeitsprozesse, Wissenssysteme und KI-gestützte Plattformökosysteme.

Dadurch entstehen strukturelle Verwundbarkeiten. Geopolitische Spannungen, Sanktionen, extraterritoriale Rechtsansprüche oder regulatorische Konflikte können unmittelbare Auswirkungen auf die operative Handlungsfähigkeit europäischer Organisationen entfalten.

Die Diskussion über digitale Souveränität darf daher nicht allein unter Datenschutz- oder Wettbewerbsaspekten geführt werden. Sie ist zunehmend auch eine Frage strategischer Resilienz und langfristiger europäischer Handlungsfähigkeit.

Diese Entwicklung spiegelt sich zunehmend auch in europäischen Regulierungsinitiativen wie der NIS2-Richtlinie wider, die digitale Infrastruktur ausdrücklich als Bestandteil strategischer Resilienz betrachtet. Die Diskussion über digitale Souveränität betrifft damit nicht mehr nur Datenschutz oder Marktstruktur, sondern zunehmend auch die langfristige operationale Handlungsfähigkeit europäischer Institutionen und Unternehmen.

Digitale Souveränität bedeutet unter diesen Bedingungen nicht technologische Autarkie. Sie bedeutet die Fähigkeit, auch unter geopolitischen Spannungen handlungsfähig zu bleiben.

1.2 Digitale Souveränität als europäische Herausforderung

Die europäische Digitalpolitik reagiert mit regulatorischen Maßnahmen, Investitionen in europäische Infrastruktur, Datenräumen, Cloud-Initiativen und dem Digital Markets Act. Diese Initiativen sind notwendig und richtig.

Sie adressieren jedoch einen zentralen strukturellen Aspekt digitaler Abhängigkeit bislang nur unzureichend:

Die praktische Interoperabilität und Wechselfähigkeit digitaler Systeme.

Die rechtlichen Rahmenbedingungen digitaler Abhängigkeit — extraterritoriale Rechtsansprüche, CLOUD Act, FISA Section 702, die strukturellen Grenzen des EU-US Data Privacy Framework — analysiert der Policy Brief Nr. 2026-001 „Digitale Souveränität in Europa“ ausführlich.[1] Er unterscheidet vier Ebenen: rechtliche Zulässigkeit, Wirksamkeit von Schutzmaßnahmen, praktische Kontrollfähigkeit und digitale Souveränität. Das vorliegende Papier vertieft die vierte Ebene in ihrer technisch-regulatorischen Dimension: die Frage, ob digitale Systeme praktisch interoperabel und damit tatsächlich ersetzbar bleiben.

[1] Illsinger, W. (2026): Digitale Souveränität in Europa. Definition, Status, Handlungsoptionen. Policy Brief Nr. 2026-001, Version 3. Wien: 4future.institute. DOI: 10.5281/zenodo.24042085.

1.3 Infrastruktur allein reicht nicht

Digitale Abhängigkeit entsteht nicht nur auf Infrastrukturebene. Sie entsteht täglich – in jedem Dokument, das nicht zuverlässig geöffnet werden kann, in jedem Kalender, der sich nicht synchronisiert, in jeder API, die proprietäre Erweiterungen voraussetzt.

Selbst wenn Daten in europäischen Rechenzentren gespeichert werden, besteht weiterhin strukturelle Abhängigkeit, wenn:

- Dokumente nicht zuverlässig zwischen unterschiedlichen Systemen austauschbar sind,
- proprietäre Erweiterungen dominante Marktstandards definieren,
- Plattformwechsel hohe operative Risiken erzeugen
- oder digitale Arbeitsprozesse nur eingeschränkt migrierbar bleiben.

Besonders sichtbar wird dies im Bereich digitaler Dokumenten- und Kollaborationssysteme. Selbst innerhalb einzelner Plattformökosysteme bestehen Unterschiede zwischen Desktop-, Web- und Mobilimplementierungen standardisierter Dokumentformate. Offene Standards wie IMAP, CalDAV oder CardDAV werden zwischen unterschiedlichen Plattformökosystemen teilweise mit unterschiedlichem Funktionsumfang und unterschiedlicher Integrationsqualität umgesetzt.

Die daraus entstehenden Interoperabilitätsrisiken wirken sich unmittelbar auf Marktentscheidungen aus. Unternehmen und öffentliche Einrichtungen orientieren sich häufig an dominanten Plattformökosystemen, weil bereits geringe Kompatibilitätsabweichungen operative und reputative Risiken erzeugen können.

Dominante Plattformökosysteme stabilisieren sich dadurch nicht ausschließlich durch Produktqualität, sondern auch durch steigende Wechselkosten und Interoperabilitätsrisiken.

1.4 Standards als unsichtbare Machtstrukturen

Standards sind die unsichtbare Infrastruktur digitaler Märkte. Sie definieren wie Systeme kommunizieren, wie Dokumente interpretiert werden, wie Daten gespeichert werden – und wie leicht oder schwer ein Plattformwechsel möglich ist.

In klassischen Industrien gelten standardisierte Schnittstellen, Zertifizierungen, Normung und überprüfbare Austauschbarkeit seit Jahrzehnten als Voraussetzung funktionierender Märkte. Beispiele wie GSM, Ethernet oder der einheitliche Ladeanschluss USB-C zeigen, dass gemeinsame — teils verbindlich vorgeschriebene — Schnittstellen Wettbewerb, Innovation und Markttransparenz fördern können.

Die Europäische Union hat diese Bedeutung in anderen Bereichen bereits erkannt: Sie hat einen einheitlichen Ladeanschluss vorgeschrieben und verpflichtet Gatekeeper nach dem Digital Markets Act zur Interoperabilität ihrer Messengerdienste.[2] Für digitale Dokumenten- und Kollaborationsökosysteme bestehen vergleichbare Anforderungen bislang nur eingeschränkt.

Dadurch entsteht ein strukturelles Problem: Formale Offenheit führt nicht automatisch zu praktischer Interoperabilität. Dominante Plattformimplementierungen definieren faktisch das reale Marktverhalten – unabhängig von formalen Spezifikationen oder Standardisierungsgremien.

Die daraus entstehenden Lock-in-Effekte beeinflussen Wettbewerb, Innovationsfähigkeit, Markteintrittsmöglichkeiten und langfristige digitale Unabhängigkeit.

[2] Richtlinie (EU) 2022/2380 (einheitliches Ladegerät); Art. 7 Verordnung (EU) 2022/1925 (Digital Markets Act).

1.5 Zielsetzung dieses Papiers

Dieses Papier knüpft an den Policy Brief Nr. 2026-001 an und vertieft dessen Abschnitt 3.2.2, der Interoperabilität als verbindliche Grundlage digitaler Souveränität definiert und CalDAV, CardDAV, IMAP sowie offene Dokumentenstandards als Mindestanforderung benennt. Es untermauert diese Forderung anhand dokumentierter Beispiele: Es zeigt, warum die formale Existenz eines Standards allein nicht ausreicht. Die Beispiele beruhen auf öffentlich dokumentierten Fällen, Herstellerdokumentation und Auskünften des Herstellersupports. Eine systematische, reproduzierbare Testreihe ersetzen sie nicht; das Papier schlägt deshalb in Kapitel 9 ein öffentliches Testkorpus vor, mit dem sich solche Befunde überprüfen lassen.

Die zentrale These lautet: Offene Standards allein sind keine ausreichende Grundlage digitaler Souveränität — weder in ihrer juristischen, noch in ihrer technologischen, noch in ihrer ökonomischen Dimension im Sinne des Policy Brief Nr. 2026-001. Entscheidend ist ihre überprüfbare und interoperable Umsetzung.

Das Papier entwickelt darauf aufbauend einen konkreten Vorschlag für:

- europäische Interoperabilitäts-Zertifizierungen,
- standardisierte Compliance-Tests,
- Referenzimplementierungen sowie
- verbindliche Interoperabilitätsanforderungen in der öffentlichen Beschaffung.

Ziel ist nicht die Einschränkung von Innovation oder Wettbewerb – sondern deren Ermöglichung. Überprüfbare Interoperabilität schafft offene, wettbewerbsfähige und resiliente digitale Märkte.

Jeder Standard ist ein guter – wenn er nur ein Standard wäre.

2 Standards als Grundlage digitaler Macht

2.1 Was Standards ermöglichen

Standards bilden die unsichtbare Infrastruktur moderner digitaler Gesellschaften. Das Internet selbst wäre ohne offene und standardisierte Protokolle wie TCP/IP, HTTP, SMTP oder DNS nicht denkbar. Auch in klassischen Industrien gelten standardisierte Schnittstellen seit Jahrzehnten als Grundlage funktionierender Märkte: Sie schaffen Austauschbarkeit, reduzieren Wechselkosten und ermöglichen Wettbewerb zwischen unterschiedlichen Herstellern.

Im digitalen Bereich erfüllen Standards jedoch nicht nur eine technische, sondern auch eine strategische Funktion. Sie bestimmen, wie leicht digitale Plattformen gewechselt werden können und wie offen oder geschlossen digitale Ökosysteme tatsächlich bleiben. Standards definieren damit nicht nur technische Kompatibilität, sondern zunehmend auch wirtschaftliche Machtverhältnisse.

Wer Standards kontrolliert, kontrolliert häufig auch den Zugang zum Markt.

2.2 Netzwerkeffekte und Plattformökonomie

Digitale Märkte unterscheiden sich strukturell von klassischen Industrien. Netzwerkeffekte führen dazu, dass dominante Systeme mit zunehmender Verbreitung immer attraktiver werden – häufig unabhängig von ihrer tatsächlichen technischen Überlegenheit.

Je stärker sich ein bestimmtes Dokumentformat, eine Kollaborationsplattform oder ein API-Ökosystem verbreitet, desto höher wird der Druck auf andere Marktteilnehmer, dieselben Systeme zu nutzen. Standards spielen dabei eine zentrale Rolle, weil sie definieren, wie kompatibel alternative Systeme mit den dominanten Plattformen bleiben.

Dadurch entstehen Märkte, in denen sich bestehende Plattformökosysteme zunehmend selbst stabilisieren. Marktkonzentration entsteht in solchen Situationen nicht ausschließlich durch Innovationsfähigkeit oder Produktqualität, sondern auch durch steigende Wechselkosten und asymmetrische Interoperabilität.

Dadurch sinkt langfristig die wettbewerbliche Dynamik digitaler Märkte. Neue Anbieter können technologische Innovationen häufig nur eingeschränkt in

Marktanteile übersetzen, wenn bestehende Plattformökosysteme durch hohe Wechselkosten strukturell abgesichert bleiben.

Besonders sichtbar wird dies im Bereich digitaler Wissensarbeit. Dokumente, Kommunikationssysteme und digitale Arbeitsprozesse müssen mit den dominanten Plattformökosystemen kompatibel bleiben, um wirtschaftliche Risiken zu vermeiden. Bereits geringe Abweichungen können operative Unsicherheiten erzeugen und wirken dadurch unmittelbar auf Marktentscheidungen zurück.

2.3 Offene vs. proprietäre Standards

Formal lassen sich digitale Standards in offene und proprietäre Standards unterscheiden. Offene Standards sind öffentlich dokumentiert und grundsätzlich von unterschiedlichen Marktteilnehmern implementierbar. Proprietäre Standards hingegen werden von einzelnen Unternehmen kontrolliert und häufig nur eingeschränkt offengelegt.

In der Praxis ist diese Unterscheidung jedoch deutlich weniger eindeutig, als sie zunächst erscheint. Auch formal offene Standards können proprietäre Erweiterungen enthalten, unterschiedlich interpretiert oder asymmetrisch implementiert werden. Ein Standard kann dadurch formal offen erscheinen und praktisch dennoch stark von einer dominanten Implementierung abhängig bleiben.

Gerade darin liegt eines der zentralen Probleme digitaler Märkte: Formale Offenheit bedeutet noch keine reale Austauschbarkeit. Die praktische Bedeutung eines Standards wird häufig weniger durch seine Spezifikation bestimmt als durch die dominante Marktimplementierung.

Diese Problematik zeigt sich heute unter anderem bei Dokumentenformaten, Kommunikationsprotokollen sowie bei Kalender- und Kontaktsynchronisation.

2.4 Open Source erzeugt nicht automatisch Wechselbarkeit

Auch Open-Source-basierte Plattformmodelle garantieren nicht automatisch langfristige Interoperabilität oder reale Wechselbarkeit.

In vielen digitalen Märkten entstehen zunehmend hybride Modelle, bei denen offene Basiskomponenten mit proprietären Erweiterungen, plattformgebundenen Cloud-Diensten oder kommerziell kontrollierten Integrationen kombiniert werden.

Dadurch können auch formal offene Ökosysteme strukturelle Abhängigkeiten erzeugen – insbesondere dann, wenn zentrale Funktionen, APIs oder organisatorische Workflows nur eingeschränkt interoperabel oder migrierbar bleiben.

Digitale Souveränität lässt sich daher weder allein über Lizenzmodelle noch über geographische Lokation definieren. Entscheidend bleibt die praktische Möglichkeit, Systeme interoperabel zu betreiben und Anbieter real wechseln zu können.

2.5 Formale Offenheit vs. praktische Interoperabilität

Die Existenz eines offenen Standards garantiert keine praktische Interoperabilität. Entscheidend ist nicht allein, ob eine Spezifikation öffentlich verfügbar ist, sondern ob unterschiedliche Implementierungen in der Praxis tatsächlich konsistent und austauschbar funktionieren.

Gerade bei komplexen Dokumenten- und Kollaborationssystemen entstehen häufig Unterschiede bei Darstellung, Layout, Kommentierung, Synchronisation oder Workflow-Verhalten. Selbst innerhalb einzelner Plattformökosysteme können Unterschiede zwischen Desktop-, Web- und Mobilimplementierungen auftreten.

Die wirtschaftliche Bedeutung solcher Unterschiede wird häufig unterschätzt. Bereits geringe Kompatibilitätsabweichungen können operative und reputative Risiken verursachen. Unternehmen und öffentliche Einrichtungen orientieren sich daher häufig an dominanten Plattformökosystemen, um genau diese Risiken zu minimieren.

Für alternative Anbieter entsteht dadurch ein strukturelles Problem: Sie tragen das wirtschaftliche Risiko möglicher Kompatibilitätsabweichungen selbst dann, wenn die Ursache der Abweichung außerhalb ihrer eigenen Implementierung liegt. Interoperabilität wird damit nicht nur zu einer technischen Herausforderung, sondern zu einem zentralen Wettbewerbsfaktor.

Auf diese Weise entstehen strukturelle Lock-in-Effekte, die bestehende Plattformdominanz zusätzlich verstärken.

2.6 Standardisierung ohne überprüfbare Konformität

Standards entfalten ihre wirtschaftliche und gesellschaftliche Wirkung nur dann vollständig, wenn ihre Implementierung konsistent erfolgt und interoperables Verhalten praktisch überprüfbar bleibt. Fehlen entsprechende Konformitätsmechanismen, entsteht eine paradoxe Situation: Standards existieren formal – ihre wettbewerbspolitische Wirkung bleibt jedoch eingeschränkt.

Das Beispiel standardisierter Dokumentformate verdeutlicht dieses Problem besonders deutlich. Office Open XML (OOXML) ist seit 2008 ein ISO-standardisierter Dokumentenstandard. Dennoch bestehen zwischen unterschiedlichen Implementierungen weiterhin erhebliche Unterschiede bei Darstellung, Layout, Kommentierung und Kollaborationsverhalten.

Die Standardisierung von OOXML erfolgte in einem politisch und wirtschaftlich intensiv diskutierten Umfeld. Kritiker verwiesen dabei unter anderem auf die Komplexität der Spezifikation, die parallele Existenz des bereits etablierten OpenDocument Formats (ODF) sowie auf die praktische Schwierigkeit interoperabler Implementierungen unterschiedlicher Office-Systeme.

Das Ergebnis ist eine Situation, in der mehrere standardisierte Dokumentenformate parallel existieren, praktische vollständige Austauschbarkeit jedoch weiterhin nur eingeschränkt erreicht wird.

Die bloße Existenz eines Standards reicht daher nicht aus, um offene Märkte sicherzustellen. Standards benötigen überprüfbare Konformität, interoperable Referenzimplementierungen und praktische Compliance-Mechanismen. Fehlen diese, bleibt Standardisierung häufig formal – ohne ihre eigentliche marktwirtschaftliche Wirkung vollständig zu entfalten.

Dabei sind zwei Fälle zu unterscheiden. Verletzt eine Implementierung verbindliche Anforderungen der Norm, ist ihr Konformitätsanspruch unberechtigt; dann muss die Implementierung korrigiert werden. Erlaubt die Norm dagegen unterschiedliche Implementierungen, die bei relevanten Anwendungen nicht zusammenpassen, gewährleistet sie die benötigte Austauschbarkeit nicht; dann muss die Norm präzisiert oder durch ein verbindliches Interoperabilitätsprofil ergänzt werden.

Für den Kunden ändert diese Unterscheidung nichts am Problem: Ein Dokument lässt sich nicht deshalb zuverlässig weiterverarbeiten, weil sein Hersteller Normkonformität erklärt. Ein Standard, der herstellerunabhängige Verarbeitung ermöglichen soll, ist an dieser Austauschbarkeit zu messen. Wie bei einer genormten Schraube gilt: Sie muss innerhalb der festgelegten Toleranzen zur genormten Mutter passen — eine „optimierte" Gewindesteigung ist mit dem Anspruch auf Normkonformität nicht vereinbar.

2.7 Der Unterschied zwischen Standardisierung und Austauschbarkeit

Standardisierung allein bedeutet noch keine reale Wechselbarkeit zwischen digitalen Plattformen. Ein Markt bleibt nur dann langfristig offen und wettbewerbsfähig, wenn Dokumente, Daten, Prozesse und digitale Arbeitsabläufe zwischen unterschiedlichen Systemen praktisch migrierbar bleiben.

Die entscheidende Frage lautet daher nicht, ob ein Standard existiert. Entscheidend ist vielmehr, ob dieser Standard reale Austauschbarkeit zwischen unterschiedlichen Plattformen ermöglicht.

In vielen digitalen Märkten besteht heute eine erhebliche Differenz zwischen formaler Standardisierung und praktischer Wechselbarkeit. Diese Differenz wird durch Netzwerkeffekte, Plattformökonomie und asymmetrische Interoperabilität zusätzlich verstärkt.

Die Sicherstellung praktischer Austauschbarkeit ist damit keine technische Detailfrage. Sie ist eine zentrale Voraussetzung digitaler Souveränität, funktionierender digitaler Märkte und langfristiger Innovationsfähigkeit.

Standards ohne überprüfbare Konformität sind keine Standards. Sie sind Versprechen.

3 Der Kampf um Dokumentstandards

3.1 Die historische Dominanz proprietärer Office-Formate

Kaum ein Bereich digitaler Infrastruktur prägt die tägliche Wissensarbeit so stark wie Dokumentenformate. Texte, Tabellen und Präsentationen bilden seit Jahrzehnten die operative Grundlage moderner Unternehmen, Verwaltungen und Bildungseinrichtungen. Dokumente enthalten nicht nur Informationen, sondern auch Geschäftsprozesse, Verträge, Entscheidungen und institutionelles Wissen.

Mit der weltweiten Verbreitung von Microsoft Office entstand seit den 1990er-Jahren faktisch ein globaler Dokumentenstandard. Formate wie DOC, XLS oder PPT wurden über viele Jahre zur dominanten Grundlage digitaler Bürokommunikation – lange bevor offene Dokumentenstandards regulatorisch oder politisch relevant wurden.

Diese Dominanz entstand nicht ausschließlich durch technische Überlegenheit. Netzwerkeffekte spielten eine zentrale Rolle: Je mehr Unternehmen und Institutionen dieselben Formate verwendeten, desto schwieriger wurde es für alternative Systeme, kompatibel zu bleiben. Dokumente mussten mit den dominanten Office-Umgebungen zuverlässig funktionieren, um operative Risiken zu vermeiden.

Dadurch entstand ein struktureller Lock-in-Effekt. Die Kontrolle über Dokumentenformate bedeutete zunehmend auch Kontrolle über digitale Arbeitsprozesse selbst.

3.2 Entstehung des OpenDocument Formats (ODF)

Mit zunehmender Bedeutung digitaler Dokumente entstand Anfang der 2000er-Jahre die politische und wirtschaftliche Forderung nach offenen, langfristig verfügbaren Dokumentstandards. Insbesondere öffentliche Einrichtungen sahen die Gefahr, dass zentrale staatliche Informationen langfristig von einzelnen proprietären Plattformen abhängig werden könnten.

Vor diesem Hintergrund entstand das OpenDocument Format (ODF), das 2006 als ISO/IEC 26300 standardisiert wurde. Ziel von ODF war es, ein vollständig offenes, dokumentiertes und herstellerunabhängiges Dokumentformat zu schaffen, das von unterschiedlichen Office-Systemen implementiert werden kann.

ODF war damit nicht nur ein technisches Projekt, sondern auch ein wirtschafts- und gesellschaftspolitisches Signal:
Dokumente sollten langfristig unabhängig von einzelnen Herstellern lesbar, austauschbar und archivierbar bleiben.

Die Diskussion um offene Dokumentenstandards entwickelte sich dadurch zunehmend zu einer Debatte über digitale Souveränität, Wettbewerb, langfristige Archivierung und die Rolle offener Standards in öffentlichen Institutionen.

3.3 Office Open XML (OOXML), die ISO-Standardisierung und das Strict/Transitional-Problem

Der politische und wirtschaftliche Kontext der OOXML-Standardisierung ist gut dokumentiert. Nachdem der US-Bundesstaat Massachusetts 2005 beschlossen hatte, für seine Verwaltung offene Dokumentformate und damit ODF vorzuschreiben,[3] und ähnliche Überlegungen in europäischen Institutionen diskutiert wurden, brachte Microsoft mit Office Open XML ein eigenes XML-basiertes Dokumentformat in den Standardisierungsprozess ein. Ecma International bildete dafür im Dezember 2005 das technische Komitee TC45, das die von Microsoft eingereichte Spezifikation zu einer Norm ausarbeiten sollte.[4] 2007 nahm auch Massachusetts Ecma-376 (Open XML) neben ODF in die Liste zulässiger Formate auf.[5]

Die anschließende ISO-Standardisierung im Schnellverfahren war international umstritten. Mehrere nationale Normungsgremien berichteten von Unregelmäßigkeiten, etwa von kurzfristigen Änderungen in der Zusammensetzung ihrer Komitees vor den Abstimmungen. Südafrika, Brasilien, Indien und Venezuela legten 2008 formelle Einsprüche ein, die ISO und IEC im August 2008 zurückwiesen.[6] In Norwegen stimmte die Normungsorganisation Standard Norge dem Format zu, obwohl die große Mehrheit ihres Fachkomitees dagegen war; im September 2008 traten 13 der 23 Komiteemitglieder aus Protest

[3] Commonwealth of Massachusetts, Information Technology Division: Enterprise Technical Reference Model (ETRM), Version 3.5, 2005; Shah, R./Kesan, J./Kennis, A. (2007): Lessons for Open Standard Policies: A Case Study of the Massachusetts Experience. University of Illinois.

[4] Ecma International, TC45 – Office Open XML Formats, https://ecma-international.org/technical-committees/tc45/; Galli, P.: Microsoft's Office Standard Gets Green Light. eWeek, 9. Dezember 2005.

[5] Commonwealth of Massachusetts, Information Technology Division: Statement on ETRM v4.0 Public Review Comments, 1. August 2007.

[6] ISO/IEC: ISO and IEC members give go ahead on ISO/IEC DIS 29500, Pressemitteilung, 15. August 2008.

zurück.[7] In Schweden erklärte die Normungsorganisation SIS ihre Abstimmung von 2007 für ungültig, nachdem bekannt geworden war, dass ein Microsoft-Mitarbeiter Partnerunternehmen Anreize für ihre Teilnahme in Aussicht gestellt hatte.[8]

OOXML wurde dennoch 2008 als ISO/IEC 29500 standardisiert.

Der Standard definiert zwei Varianten: „Strict" als die bereinigte Fassung ohne die Übergangsfunktionen und „Transitional" als Variante für den Übergang bestehender Dokumente aus älteren Microsoft-Office-Formaten. Transitional entspricht weitgehend jener Fassung, die in der Abstimmung vom September 2007 keine Mehrheit gefunden hatte, und war nicht für neue Dokumente gedacht. In der Praxis blieb Transitional dennoch über viele Jahre die dominierende Implementierung — nicht nur bei Drittanbietern, sondern bei Microsoft selbst.

Alex Brown, der 2008 das Ballot Resolution Meeting der ISO geleitet und die Standardisierung verteidigt hatte, warf Microsoft 2010 öffentlich vor, die gegenüber der internationalen Normungsgemeinschaft eingegangenen Zusagen zu brechen: Die Vorabversion von Office 2010 unterstütze „nicht die genehmigte Strict-Variante", sondern das 2007 abgelehnte Format.[9] Microsoft kündigte daraufhin an, Strict ab der folgenden Office-Version lesen und schreiben zu können. Seit Office 2013 ist das möglich; als Standardformat speichert Office jedoch bis heute Transitional.[10]

Transitional ist Bestandteil der verabschiedeten Norm ISO/IEC 29500; wer es verwendet, verlässt die Norm nicht. Die Kritik richtet sich gegen die Wirkung: Eine als Übergang gedachte Variante ist zum Normalfall geworden und trägt herstellerspezifische Altlasten fort. Schon der Name sagt, was gemeint war. Nach der Begründung im Normungsverfahren sollten die Übergangsfunktionen einen Übergangszeitraum ermöglichen, in dem bestehende Dokumente bei der Migration ihre Darstellung behalten; neue Dokumente sollten sie nicht

[7] Norway ISO members walk out over OOXML. iTnews, Oktober 2008; https://arstechnica.com/uncategorized/2008/10/norwegian-standards-body-implodes-over-ooxml-controversy/

[8] https://www.computerworld.com/article/1581527/microsoft-admits-swedish-employee-promised-incentives-for-open-xml-support.html

[9] Brown, A.: Microsoft Fails the Standards Test. Blog, 31. März 2010, https://adjb.net/posts/ms-fail/ (Zitat in eigener Übersetzung).

[10] Mahugh, D.: Office's Support for ISO/IEC 29500 Strict. Microsoft-Blog, 6. April 2010, https://learn.microsoft.com/en-us/archive/blogs/dmahugh/offices-support-for-isoiec-29500-strict; Office 2013 to support Strict Open XML. The Register, 15. August 2012.

verwenden.[11] Seit der Verabschiedung 2008 sind fast zwei Jahrzehnte vergangen. Ein Übergang, der so lange dauert und in dem neue Dokumente weiterhin standardmäßig im Übergangsformat entstehen, ist kein Übergang mehr, sondern der Dauerzustand. Teil 4 der Norm (Transitional Migration Features) enthält etwa Kompatibilitätseinstellungen wie autoSpaceLikeWord95 oder lineWrapLikeWord6, die das Verhalten historischer Word-Versionen nachbilden sollen. In der Ecma-Fassung von 2006 hieß es dazu noch, dieses Verhalten lasse sich nicht vollständig beschreiben; Anwendungen müssten die Ausgabe der historischen Anwendung nachbilden. Im ISO-Verfahren wurden diese Einstellungen ausführlicher beschrieben und als nicht für neue Dokumente bestimmt gekennzeichnet.[12]

Hinzu kommt die Herstellerdokumentation. Microsoft beschreibt in einer eigenen, laufend aktualisierten Spezifikation, wo Office ISO/IEC 29500 anders umsetzt oder ergänzt, und dokumentiert in weiteren Spezifikationen Word-, Excel- und PowerPoint-Erweiterungen des Formats.[13] Diese Offenlegung ist für andere Implementierungen hilfreich. Sie zeigt aber auch, dass die Norm allein als gemeinsame Implementierungsgrundlage nicht ausreicht: Wer mit Microsoft Office zuverlässig Dokumente austauschen will, muss neben ISO/IEC 29500 die Herstellerspezifikationen und das tatsächliche Produktverhalten berücksichtigen.

Dokumentierte Einzelfälle zeigen, was das praktisch bedeutet:

[11] Antwort der Ecma TC45 im ISO-Verfahren, wiedergegeben in: Jones, B.: suppressTopSpacingWP – Compat Settings #1. Microsoft-Blog, 2008, https://learn.microsoft.com/en-us/archive/blogs/brian_jones/suppresstopspacingwp-compat-settings-1

[12] Ecma-376, 1. Ausgabe (2006), Teil 4, Abschnitt 2.15.3.6 (autoSpaceLikeWord95); ISO/IEC 29500-4:2008, Transitional Migration Features, Abschnitt 9.7.3 (Compatibility Settings); Jones, B.: suppressTopSpacingWP – Compat Settings #1. Microsoft-Blog, 2008.

[13] Microsoft Open Specifications: [MS-OI29500] Office Implementation Information for ISO/IEC 29500 Standards Support; [MS-DOCX] Word Extensions to the Office Open XML (.docx) File Format; [MS-XLSX]; [MS-PPTX], https://learn.microsoft.com/en-us/openspecs/office_standards/

- **Abweichung zwischen Norm und Produktverhalten:** Laut Norm sollen bei einem Formularfeld ohne Eigenschaftsangaben (ffData) Standardwerte gelten; Word behandelt ein solches Feld nach Microsofts eigener Dokumentation als ungültig, es kann weder genutzt noch bearbeitet werden. Die in der Norm vorgesehenen Unterelemente label und tabIndex ignoriert Word und speichert sie nicht mit. Feldnamen dürfen laut Norm bis zu 65 Zeichen lang sein, in Word höchstens 20.[14]
- **Herstellerspezifische Layoutregeln:** Ob bei einer Silbentrennung am Seiten- oder Spaltenende nur das letzte Wort oder die ganze letzte Zeile auf die nächste Seite rückt, steuert Word über die Einstellungen allowHyphenationAtTrackBottom und useWord2013TrackBottomHyphenation in einem Microsoft-eigenen Namensraum, dokumentiert in [MS-DOCX]. LibreOffice hat diese Einstellungen 2024 eigens nachgebaut: Das Testdokument im zugehörigen Fehlerbericht setzt Word auf drei Seiten, LibreOffice setzte es vor der Korrektur auf zwei.[15]
- **Versionsabhängiges Verhalten:** Bei einem Bild mit quadratischem Textumfluss, das relativ zur Spalte zentriert ist und bei dem Text nur auf der größeren Seite fließen soll, ordnet Word den Text seit Version 2013 auf der anderen Seite an als in älteren Versionen. Dasselbe DOCX-Dokument erschien deshalb in Collabora Online und Word unterschiedlich.[16] In einem älteren Fehlerbericht von 2020 bezeichnete ein LibreOffice-Entwickler die Nachbildung des Layouts ab Word 2013 als Notlösung für einen Layoutfehler in Word, den Microsoft besser selbst beheben solle — eine fachliche Einschätzung dieses Entwicklers, keine festgestellte Ursache aller Probleme beim Textumfluss.[17]

Diese Fälle beweisen keine Behinderungsabsicht, und nicht jeder belegt eine Normverletzung Microsofts. Sie belegen aber den Mechanismus: Wer DOCX-

[14] Microsoft: [MS-OI29500], Abschnitt 2.1.518 (Part 1 Section 17.16.17, ffData) und 2.1.538 (Part 1 Section 17.18.26, ST_FFName), https://learn.microsoft.com/en-us/openspecs/office_standards/ms-oi29500/

[15] Microsoft: [MS-DOCX], Abschnitte 2.3.7 und 2.3.8; LibreOffice Bugzilla, Fehler 160518 („DOCX: fix layout of hyphenated text by supporting allowHyphenationAtTrackBottom and useWord2013TrackBottomHyphenation"), behoben in Version 24.8; Vergleich anhand der Testdatei in Anhang 193486 (useWord2013TrackBottomHyphenation = 1, allowHyphenationAtTrackBottom = 0): in Word drei Seiten, in LibreOffice vor der Korrektur zwei. Spätere Ergänzungen zum Export behandelt Fehler 165354.

[16] Collabora-Online-Forum: There is a significant difference in how the same DOCX document is rendered in Collabora Online versus Microsoft Office, Thread 4664, 2026.

[17] LibreOffice Bugzilla, Fehler 134509 („FILEOPEN DOCX: Text behind image"), Kommentar 12 vom 2. Dezember 2020.

Dokumente zuverlässig mit Word austauschen will, muss neben der Norm Herstellerspezifikationen, versionsabhängiges Produktverhalten und fortlaufende Kompatibilitätskorrekturen berücksichtigen. Die Dateiendung DOCX beschreibt allein noch keine einheitliche Erwartung an die Darstellung.

Die strukturelle Konsequenz ist eindeutig: Alternative Anbieter tragen zusätzlichen Anpassungsaufwand, um das Verhalten der marktbeherrschenden Implementierung nachzubilden, und Kunden erleben verbleibende Abweichungen als Risiko eines Anbieterwechsels. Dafür muss nicht belegt werden, dass Abweichungen gezielt geschaffen wurden — entscheidend ist der Mechanismus. Der faktische Referenzstandard ist nicht ISO/IEC 29500 Strict, sondern das Verhalten von Microsoft Office.

Die parallele Existenz von ODF und OOXML als ISO-Standards hat die erhoffte Interoperabilität nicht hergestellt. Sie hat die Komplexität erhöht – und die strukturelle Abhängigkeit von der dominanten Implementierung verstärkt.

3.4 Warum Dokumentstandards über digitale Souveränität entscheiden

Dokumentenstandards sind keine technische Randfrage. Sie bestimmen, wie Wissen gespeichert, ausgetauscht und langfristig nutzbar bleibt.

Wenn Dokumente:

- nicht zuverlässig zwischen unterschiedlichen Systemen austauschbar sind,
- nur eingeschränkt migriert werden können
- oder bestimmte Plattformen faktisch bevorzugen,

entstehen tiefgreifende strukturelle Abhängigkeiten.

Besonders relevant wird dies in öffentlichen Institutionen und Unternehmen mit langfristigen Archivierungs- und Dokumentationspflichten. Dokumente müssen dort häufig:

- über Jahrzehnte lesbar bleiben,
- zwischen unterschiedlichen Systemen migriert werden können
- und unabhängig von einzelnen Herstellern verfügbar bleiben.

Fehlende praktische Interoperabilität führt hingegen zu:

- steigenden Wechselkosten,
- langfristigen Plattformabhängigkeiten
- und eingeschränkter Wettbewerbsoffenheit.

Dokumentenstandards werden damit zu einer zentralen infrastrukturellen Frage digitaler Souveränität.

3.5 Langzeitarchivierung und staatliche Abhängigkeiten

Die Bedeutung offener und interoperabler Dokumentstandards zeigt sich besonders deutlich im Bereich der Langzeitarchivierung staatlicher und institutioneller Informationen.

Staatliche Dokumente, Verträge, Verwaltungsakten oder wissenschaftliche Arbeiten müssen häufig über Jahrzehnte oder sogar Jahrhunderte lesbar bleiben. Proprietäre oder nur eingeschränkt interoperable Formate erzeugen dabei erhebliche Risiken:

- zukünftige Softwareabhängigkeiten,
- eingeschränkte Migrationsfähigkeit,
- Verlust von Formatierungs- oder Metadaten
- sowie langfristige Kontrollverluste über öffentliche Informationen.

Digitale Souveränität bedeutet daher nicht nur Kontrolle über Infrastruktur und Datenstandorte. Sie bedeutet auch:
die langfristige Fähigkeit, eigene Informationen unabhängig von einzelnen Plattformökosystemen lesen, migrieren und archivieren zu können.

Gerade öffentliche Institutionen tragen hier eine besondere Verantwortung. Ihre Beschaffungsentscheidungen beeinflussen nicht nur kurzfristige Produktivität, sondern langfristig auch:

- Marktstrukturen,
- Wettbewerb
- und die digitale Resilienz staatlicher Informationssysteme.

4 Asymmetrische Interoperabilität in der Praxis

4.1 Wenn Standards nur „teilweise offen“ sind

Die Existenz offener Standards vermittelt häufig den Eindruck technischer Neutralität und Austauschbarkeit. In der Praxis zeigt sich jedoch, dass Interoperabilität selten vollständig funktioniert. Systeme sind meist weder vollständig offen noch vollständig geschlossen. Stattdessen entstehen hybride Plattformökosysteme, in denen Standards formal unterstützt werden, ihre praktische Umsetzung jedoch erhebliche Unterschiede aufweist.

Gerade in digitalen Plattformmärkten genügt bereits eine teilweise asymmetrische Interoperabilität, um starke Lock-in-Effekte zu erzeugen. Systeme funktionieren grundsätzlich miteinander – allerdings nicht gleichwertig. Bestimmte Funktionen bleiben eingeschränkt, Integrationen unvollständig oder Benutzererfahrungen inkonsistent.

Dadurch entsteht eine strukturelle Marktasymmetrie: Die dominante Plattform bietet innerhalb ihres eigenen Ökosystems die vollständigste und risikoärmste Nutzererfahrung, während alternative Anbieter trotz Standardunterstützung häufig als „nicht vollständig kompatibel“ wahrgenommen werden.

Interoperabilität wird dadurch formal zugesichert, praktisch jedoch graduell begrenzt.

4.2 E-Mail: IMAP als Second-Class Citizen

IMAP („Internet Message Access Protocol“) ist seit Jahrzehnten ein offener Standard für den Zugriff auf E-Mail-Postfächer. Es wurde 1988 erstmals als RFC 1064 beschrieben; die heutige Fassung IMAP4rev2 ist in RFC 9051 (2021) spezifiziert, die Vorgängerversion IMAP4rev1 in RFC 3501 (2003).[18] Der Standard wird von der Internet Engineering Task Force (IETF) gepflegt und bildet bis heute eine zentrale Grundlage interoperabler E-Mail-Kommunikation.

Gleichzeitig zeigt sich gerade im Bereich moderner Plattformökosysteme, dass formale Standardunterstützung nicht automatisch gleichwertige Funktionalität bedeutet.

[18] RFC 1064 (1988); RFC 3501 (2003); Melnikov, A./Leiba, B.: RFC 9051, Internet Message Access Protocol (IMAP) – Version 4rev2, 2021.

Der seit 2023 schrittweise eingeführte neue Outlook für Windows unterstützt IMAP- und POP-Konten, behandelt sie aber anders als Exchange- oder Microsoft-365-Konten. Funktionen wie Kalenderintegration, die Verarbeitung von Besprechungseinladungen oder plattformübergreifende Zusammenarbeit stehen für IMAP-Konten nur eingeschränkt zur Verfügung.[19]

Auf der offiziellen Supportplattform Microsoft Q&A verweisen Supportmitarbeiter Nutzer, die mit IMAP-Konten Besprechungseinladungen verwalten wollen, an den klassischen Outlook-Client oder an eine Migration des Postfachs zu Microsoft 365. Begründet wird dies damit, dass IMAP und POP nur die Synchronisation von E-Mails unterstützen, nicht die eines vollständigen Kalenders.[20] Das trifft auf IMAP zu — der offene Standard für Kalender ist CalDAV. Diesen unterstützt Outlook nicht (siehe Abschnitt 4.3).

So werden Kalendereinladungen bei IMAP-Konten im neuen Outlook in einem lokalen Kalender des jeweiligen Kontos abgelegt, der nicht mit anderen Kalendern oder Geräten synchronisiert wird.[21] Für Nutzer entsteht dadurch eine asymmetrische Benutzererfahrung:

Das Beispiel verdeutlicht ein grundlegendes Muster moderner Plattformmärkte: Standards werden formal unterstützt, praktisch jedoch unterschiedlich tief in das jeweilige Plattformökosystem integriert. Interoperabilität bleibt dadurch bestehen – allerdings nicht gleichwertig.

4.3 Kalender und Kontakte: CalDAV und CardDAV in proprietären Ökosystemen

CalDAV und CardDAV sind offene Standards für Kalender- und Kontaktsynchronisation, spezifiziert in RFC 4791 (2007) und RFC 6352 (2011) der Internet Engineering Task Force (IETF).[22] Sie werden unter anderem von Apple Kalender, Google Kalender, Thunderbird und der überwiegenden Mehrheit anderer E-Mail- und Kalender-Clients nativ unterstützt.

[19] Microsoft Support: Feature comparison between new Outlook and classic Outlook, laufend aktualisiert, https://support.microsoft.com/office/de453583-1e76-48bf-975a-2e9cd2ee16dd

[20] Microsoft Q&A, Frage 5853986 („Why does the new Outlook no longer support my email…"), Antwort aus dem Microsoft-Support, https://learn.microsoft.com/en-us/answers/questions/5853986/

[21] Microsoft Q&A, „New Outlook – non-MSA account calendar invites do not save to default calendar", 27. Januar 2026, https://learn.microsoft.com/en-us/answers/questions/5742426/

[22] Daboo, C./Desruisseaux, B./Dusseault, L.: RFC 4791, Calendaring Extensions to WebDAV (CalDAV), 2007; Daboo, C.: RFC 6352, CardDAV: vCard Extensions to WebDAV, 2011.

Microsoft Outlook unterstützt CalDAV und CardDAV weder im klassischen noch im neuen Client nativ. Auf Microsoft Q&A empfahl der Microsoft-Support im Januar 2026 Nutzern, die auf CalDAV angewiesen sind, zum klassischen Outlook zurückzukehren und dort die Erweiterung „CalDav Synchronizer" eines Drittanbieters zu verwenden.[23]

Diese fehlende native Unterstützung besitzt erhebliche strukturelle Auswirkungen auf digitale Arbeitsökosysteme.

Outlook ist in vielen Unternehmen und öffentlichen Institutionen der zentrale E-Mail- und Kalender-Client. Gleichzeitig erreicht die Plattform ihre höchste Integrationstiefe innerhalb des Microsoft-365-Ökosystems. Systeme die auf offenen Standards wie CalDAV und CardDAV basieren, können diese Integrationsqualität innerhalb von Outlook hingegen nur eingeschränkt erreichen.

Die erwähnte Erweiterung, „Outlook CalDav Synchronizer", ist ein Open-Source-Projekt der Wiener Generalize-IT Solutions OG, das die fehlende Synchronisation für den klassischen Outlook-Client nachrüstet.[24] Für den neuen Outlook-Client steht sie nicht zur Verfügung, weil dieser keine klassischen COM-Add-ins unterstützt. Mit der Ablösung des klassischen Clients verliert damit auch diese Brücke zu offenen Standards ihre Grundlage.

Microsoft dokumentiert für Outlook keine native Unterstützung von CalDAV oder CardDAV. Entsprechende Nutzeranfragen finden sich seit vielen Jahren auf offiziellen Support- und Communityplattformen, ohne dass eine native Implementierung angekündigt oder dokumentiert wurde.

Die fehlende Unterstützung offener Kalender- und Kontaktstandards wird dabei nicht explizit als Ablehnung kommuniziert. Praktisch entsteht jedoch eine Situation, in der plattformeigene Integrationsmechanismen kontinuierlich weiterentwickelt werden, während offene Standardprotokolle innerhalb des dominanten Plattformökosystems keine gleichwertige Unterstützung erhalten.

[23] Microsoft Q&A, „New Outlook – non-MSA account calendar invites do not save to default calendar", Antwort der Moderation („Microsoft External Staff") vom 27. Januar 2026, https://learn.microsoft.com/en-us/answers/questions/5742426/

[24] Outlook CalDav Synchronizer, Open-Source-Projekt (AGPL) der Generalize-IT Solutions OG, Wien, https://github.com/aluxnimm/outlookcaldavsynchronizer

Parallel dazu zeigt Exchange ActiveSync (EAS) – das proprietäre Microsoft-Protokoll für mobile E-Mail- und Kalendersynchronisation – ein komplementäres Muster. EAS ist ein von Microsoft kontrolliertes und lizenziertes Protokoll, das von zahlreichen Plattformen und mobilen Clients implementiert wurde, um Kompatibilität mit Exchange- und Microsoft-365-Umgebungen sicherzustellen.

Microsofts eigene Desktop-Clients setzen jedoch kaum noch auf EAS. Für Verbindungen zu Exchange Server unterstützt Outlook EAS nach Microsofts Angaben nicht; EAS ist dort nur für andere Dienste vorgesehen.[25] Für eben diese anderen Dienste schränkte ein Update von Outlook 2016 (Version 16.0.8431.2079 vom 12. September 2017) die Einrichtung ein: Mit der neu eingeführten vereinfachten Kontoeinrichtung scheitert nach Berichten von Anbietern EAS-fähiger Mailserver das Anlegen neuer EAS-Konten auf dem üblichen Weg. Bereits eingerichtete Konten funktionieren weiter; die frühere Einrichtung lässt sich nur durch einen Eingriff in die Windows-Registrierung wiederherstellen, der die vereinfachte Kontoeinrichtung abschaltet.[26] Die Funktion ist also vorhanden, für neue Konten aber nur noch über Umwege nutzbar. Der neue Outlook für Windows unterstützt EAS-Konten überhaupt nicht.[27]

Dadurch entsteht eine strukturell asymmetrische Situation:
Offene Standards werden branchenweit unterstützt, jedoch nicht nativ innerhalb des dominanten Outlook-Ökosystems integriert. Proprietäre Microsoft-Protokolle wiederum wurden von großen Teilen der Industrie implementiert, verlieren innerhalb moderner Microsoft-Plattformarchitekturen jedoch selbst an Bedeutung.

Die eigentliche Plattformbindung entsteht damit nicht primär durch fehlende Standardisierung, sondern durch unterschiedliche Qualität und Tiefe der Integration. Für Organisationen entsteht ein praktischer Anreiz, das vollständig integrierte Plattformökosystem zu verwenden, um operative Reibungsverluste und Kompatibilitätsprobleme zu vermeiden.

[25] Microsoft Learn: Outlook doesn't support connections to Exchange by using ActiveSync (ursprünglich KB 2859522), gilt für Outlook 2013, 2016 und 2019, https://learn.microsoft.com/en-us/troubleshoot/outlook/profiles-and-accounts/outlook-cannot-use-activesync-connect-exchange

[26] SmarterTools: Microsoft Outlook 2016 and EAS, 4. Oktober 2017, https://smartertools.com/blog/2017/10/04-Outlook-2016-and-EAS

[27] Microsoft Q&A: How to use other Exchange ActiveSync account in Win11, Antwort aus dem Microsoft-Support, https://learn.microsoft.com/en-us/answers/questions/1827479/

Interoperabilität bleibt formal bestehen. Praktisch verliert sie jedoch ihre Gleichwertigkeit gegenüber tief integrierten proprietären Plattformdiensten.

4.4 Proprietäre Erweiterungen, APIs und migrationsinduzierte Plattformbindung

Ein zentrales Muster asymmetrischer Interoperabilität besteht nicht in der vollständigen Ablehnung offener Standards, sondern in deren selektiver Implementierung kombiniert mit proprietären Erweiterungen, die innerhalb des dominanten Plattformökosystems strukturelle Vorteile erzeugen.

Dieses Muster zeigt sich bei:

- Dokumentformaten,
- Kommunikationsprotokollen,
- Kalenderstandards
- und zunehmend auch bei programmatischen Schnittstellen (APIs), die den Zugriff auf Plattformdaten und Dienste definieren.

Das dokumentierte Beispiel: EWS und Microsoft Graph

Exchange Web Services (EWS) war seit 2007 die zentrale Schnittstelle für den programmatischen Zugriff auf Exchange-Postfächer. Zahlreiche Drittanbieter-Produkte – darunter Backup-Lösungen, CRM-Systeme, Kalender-Clients und Kollaborationsplattformen – wurden auf Basis dieser Schnittstelle entwickelt.

2018 stellte Microsoft die funktionale Weiterentwicklung von EWS ein. 2023 kündigte das Unternehmen an, EWS in Exchange Online abzuschalten. Nach dem aktualisierten Zeitplan vom Februar 2026 wird EWS seit 1. Oktober 2026 schrittweise deaktiviert; Organisationen können es nur noch über eine Ausnahmeliste für einzelne Anwendungen weiter nutzen. Ab 1. April 2027 wird EWS in Exchange Online endgültig und ohne Ausnahmen abgeschaltet.[28] Exchange Server im eigenen Rechenzentrum ist nicht betroffen. Als Nachfolger benennt Microsoft die Microsoft Graph API.

Microsoft Graph ist keine Weiterentwicklung eines offenen Standards, sondern eine proprietäre REST-basierte Plattform-API unter Kontrolle von Microsoft – mit

[28] Microsoft 365 Message Center, MC1227454: Exchange Web Services (EWS) retirement update, 5. Februar 2026; Microsoft Learn: Deprecation of Exchange Web Services in Exchange Online, https://learn.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-ews-exchange-online

eigenem Authentifizierungsmodell, eigenem Berechtigungssystem und plattformspezifischen Zugriffskonzepten.

Microsoft selbst spricht von „nahezu vollständiger" Funktionsparität zwischen Graph und EWS; bestimmte Funktionen stehen über Graph nicht oder nur in anderer Form zur Verfügung.

Die strukturelle Folge ist technisch und wirtschaftlich relevant:
Drittanbieter, die ihre Produkte über viele Jahre auf einer dokumentierten Schnittstelle aufgebaut haben, müssen innerhalb eines fixen Zeitfensters auf eine proprietäre Plattform-API migrieren – bei dokumentierten funktionalen Unterschieden und ohne standardisierte interoperable Alternative.

Das Muster in seiner allgemeinen Form

EWS ist dabei kein Einzelfall, sondern Ausdruck eines allgemeinen Plattformmusters:
Dokumentierte oder offene Schnittstellen werden schrittweise durch proprietäre Plattformarchitekturen ersetzt. Die daraus entstehenden Migrationen erzeugen:

- technische Umstellungskosten,
- organisatorische Abhängigkeiten
- und steigende Integrationskomplexität.

Proprietäre Erweiterungen betreffen dabei längst nicht mehr nur Dokumentformate oder Kommunikationsprotokolle. Sie umfassen zunehmend:

- Workflow-Logiken,
- Metadaten,
- Kollaborationsmechanismen,
- Authentifizierungsmodelle
- und plattformspezifische Integrationen.

Je komplexer digitale Arbeitsumgebungen werden, desto schwieriger wird die Nachbildung dieser Integrationen durch alternative Anbieter. Der eigentliche Wettbewerbsnachteil entsteht dadurch häufig nicht bei der Implementierung des Standards selbst, sondern bei der Nachbildung des proprietären Plattformverhaltens das den Standard umgibt.

Interoperabilität bleibt formal bestehen. Die strukturelle Asymmetrie entsteht in der Schicht darüber.

4.5 „S3-kompatibel“ und andere Illusionen der Austauschbarkeit

Besonders deutlich zeigt sich die Problematik asymmetrischer Interoperabilität bei sogenannten „kompatiblen“ Plattformdiensten. Ein bekanntes Beispiel ist der Begriff „S3-kompatibel“.

Amazon S3 („Simple Storage Service“) entwickelte sich in den vergangenen Jahren faktisch zum De-facto-Standard für objektbasierten Cloud-Speicher. Zahlreiche europäische und internationale Anbieter werben heute mit „S3-Kompatibilität“, um die Austauschbarkeit ihrer Speicherlösungen mit bestehenden Cloud-Anwendungen zu signalisieren.

In der Praxis bedeutet diese Kompatibilität jedoch häufig lediglich grundlegende API-Funktionalität – nicht zwingend vollständige Gleichwertigkeit bei:

- Berechtigungsmodellen,
- Metadaten,
- Performance,
- Replikation,
- Sicherheitsfunktionen
- oder Workflow-Integration.

Gerade in komplexen Unternehmensumgebungen können bereits kleine Unterschiede erhebliche operative Auswirkungen haben.

Dadurch entsteht eine Situation, in der alternative Anbieter formal kompatibel erscheinen, die dominante Plattform jedoch weiterhin als risikoärmste Referenzimplementierung wahrgenommen wird.

Die Folge ist ein strukturell verzerrter Markt: Interoperabilität existiert formal, reale Wechselbarkeit bleibt jedoch eingeschränkt.

Asymmetrische Interoperabilität wird damit zu einem zentralen Mechanismus moderner Plattformökonomie.

5 Kollaborationsplattformen als neue Abhängigkeit

5.1 Vom Dokument zur Plattform

Die digitale Abhängigkeit moderner Arbeitsumgebungen entsteht heute nicht mehr ausschließlich auf Ebene einzelner Dokumentformate. Während sich frühere Lock-in-Effekte primär auf Dateien und proprietäre Formate konzentrierten, verlagert sich Plattformmacht zunehmend auf integrierte digitale Arbeitsökosysteme.

Dokumente sind heute nur noch ein Bestandteil komplexer Kollaborationsplattformen. Kommunikation, Kalender, Identität, Dateiablage, Videokonferenzen, Aufgabenverwaltung, Berechtigungen und Workflow-Systeme werden zunehmend in einheitlichen Plattformumgebungen zusammengeführt.

Dadurch verändert sich auch die Struktur digitaler Abhängigkeit:
Nicht mehr einzelne Dateien stehen im Mittelpunkt, sondern komplette digitale Arbeitsprozesse.

Der Wechsel eines Plattformökosystems betrifft damit nicht nur Dokumente, sondern:

- Kommunikation,
- Zusammenarbeit,
- Identitätsmanagement,
- Prozesslogiken
- und organisatorische Abläufe.

Die Wechselkosten steigen dadurch erheblich (siehe Abbildung 1).



Abbildung 1: Evolution digitaler Plattformen

5.2 Teams, SharePoint und integrierte Arbeitsökosysteme

Moderne Kollaborationsplattformen entwickeln ihre Stärke vor allem durch tiefe Integration. Systeme wie Microsoft Teams, SharePoint oder vergleichbare Plattformlösungen verbinden:

- Kommunikation,
- Dateiablage,
- Rechteverwaltung,
- Meetings,
- Kollaboration
- und Workflow-Logiken

zu einem einheitlichen digitalen Arbeitsraum.

Innerhalb solcher Plattformen entsteht eine konsistente und hochintegrierte Benutzererfahrung. Gleichzeitig wird Interoperabilität mit externen oder alternativen Systemen zunehmend komplex.

Dokumente sind dabei nur noch ein Teil eines wesentlich größeren Plattformkontexts:

- Berechtigungen,
- Kommentare,
- Versionshistorien,
- Freigaben,
- Meetings,
- Automatisierungen
- und KI-Funktionen

werden direkt mit dem Plattformökosystem verknüpft.

Dadurch entsteht eine neue Form digitaler Abhängigkeit:
Die eigentliche Bindung erfolgt nicht mehr primär über Dokumentformate, sondern über integrierte Arbeitsumgebungen.

5.3 Workflow-Lock-in statt Dateiformat-Lock-in

Mit der zunehmenden Integration digitaler Arbeitsprozesse verschiebt sich auch die Natur von Lock-in-Effekten. Während frühere Abhängigkeiten vor allem auf proprietären Dateiformaten beruhten, entstehen moderne Wechselbarrieren zunehmend auf Ebene:

- von Workflows,
- Integrationen,
- Automatisierungen
- und Kollaborationslogiken.

Je stärker Unternehmen ihre Arbeitsprozesse an ein bestimmtes Plattformökosystem anpassen, desto schwieriger wird ein späterer Wechsel.

Besonders relevant wird dies bei:

- automatisierten Prozessen,
- KI-gestützten Workflows,
- integrierter Rechteverwaltung,
- Kommunikationshistorien
- oder plattformspezifischen Erweiterungen.

Die eigentliche Herausforderung liegt dabei weniger in der Migration einzelner Datenbestände als in der Wiederherstellung funktionaler organisatorischer Abläufe innerhalb eines neuen Systems.

Lock-in entsteht dadurch zunehmend auf semantischer und organisatorischer Ebene – nicht nur auf technischer Ebene.

5.4 Identität, Kommunikation und proprietäre Integration

Ein wesentlicher Bestandteil moderner Plattformökosysteme ist die zentrale Integration von Identität und Kommunikation. Benutzerkonten, Zugriffsrechte, Gruppenstrukturen, Kalender, Chats, Meetings und Kollaborationsfunktionen werden dabei eng miteinander verbunden.

Dadurch entstehen hochintegrierte digitale Arbeitsumgebungen, deren Wert nicht primär in einzelnen Anwendungen liegt, sondern in der Gesamtheit ihrer Integrationen.

Für alternative Anbieter entsteht daraus eine erhebliche Herausforderung: Selbst wenn einzelne Funktionen interoperabel oder standardbasiert verfügbar sind, bleibt die vollständige Integration häufig plattformspezifisch.

Die Folge ist eine asymmetrische Interoperabilität:
Alternative Systeme können häufig grundlegende Funktionen bereitstellen,

erreichen jedoch nicht dieselbe Integrationstiefe und Konsistenz innerhalb des dominanten Plattformökosystems.

Gerade dadurch entstehen langfristige Abhängigkeiten, die weit über einzelne Softwareprodukte hinausgehen.

5.5 Warum Wechselkosten mit jeder Integration wachsen

Die wirtschaftliche Bedeutung moderner Plattformökosysteme liegt vor allem in ihrer Fähigkeit, Wechselkosten kontinuierlich zu erhöhen.

Die wirtschaftswissenschaftliche Forschung beschreibt, wie Wechselkosten und Netzwerkeffekte etablierte Anbieter absichern und Märkte zugunsten eines Systems kippen lassen können.[29] In integrierten Plattformökosystemen kommt hinzu, dass sich Bindungen über viele Dienste hinweg aufsummieren.

Mit jeder zusätzlichen Integration wachsen:

- technische Abhängigkeiten,
- organisatorische Anpassungen,
- Schulungsaufwand,
- Datenmigrationen
- und prozessuale Bindungen.

Gleichzeitig steigt die Komplexität interoperabler Alternativen. Selbst wenn einzelne Komponenten technisch ersetzt werden könnten, bleibt die Wiederherstellung vergleichbarer organisatorischer Abläufe häufig mit erheblichen Risiken verbunden.

Besonders problematisch ist dabei die kumulative Wirkung dieser Abhängigkeiten. Einzelne Integrationen erscheinen oft unkritisch. Über Jahre entsteht jedoch ein hochkomplexes Plattformökosystem, dessen vollständige Migration wirtschaftlich und organisatorisch zunehmend unrealistisch wird.

Dadurch verlagert sich digitale Marktmacht schrittweise:
von einzelnen Anwendungen hin zu integrierten digitalen Arbeitswelten.

[29] Farrell, J./Klemperer, P. (2007): Coordination and Lock-In: Competition with Switching Costs and Network Effects. In: Armstrong, M./Porter, R. (Hg.): Handbook of Industrial Organization, Bd. 3. Amsterdam: Elsevier, S. 1967–2072.

Interoperabilität wird unter diesen Bedingungen nicht nur zu einer technischen Eigenschaft einzelner Produkte, sondern zu einer zentralen Voraussetzung funktionierender digitaler Märkte.

6 Der blinde Fleck des Digital Markets Act (DMA)

6.1 Ziele und Mechanismen des DMA

Mit dem Digital Markets Act (DMA) hat die Europäische Union erstmals versucht, die strukturelle Marktmacht großer digitaler Plattformen regulatorisch zu adressieren. Ziel des DMA ist es, faire Wettbewerbsbedingungen in digitalen Märkten zu schaffen und die Abhängigkeit von sogenannten „Gatekeepern" zu begrenzen.

Der DMA richtet sich an Plattformunternehmen, die aufgrund ihrer Größe, Reichweite und Marktstellung eine zentrale Vermittlerrolle zwischen Unternehmen und Endnutzern einnehmen. Die Regulierung soll verhindern, dass dominante Plattformen ihre Marktstellung nutzen, um Wettbewerb systematisch einzuschränken oder alternative Anbieter strukturell zu benachteiligen.

Zu den zentralen Mechanismen des DMA zählen unter anderem:

- Interoperabilitätsanforderungen,
- Datenportabilität,
- Einschränkungen plattforminterner Selbstbevorzugung
- sowie Verpflichtungen zur Öffnung bestimmter Schnittstellen.

Der DMA markiert damit einen wichtigen regulatorischen Paradigmenwechsel: Digitale Märkte werden nicht länger ausschließlich als Innovationsräume betrachtet, sondern zunehmend auch als infrastrukturelle Machtstrukturen.

6.2 Gatekeeper-Regulierung und ihre Grenzen

Trotz seiner Bedeutung weist der DMA erhebliche strukturelle Grenzen auf. Die Regulierung konzentriert sich primär auf:

- Suchmaschinen,
- App Stores,
- soziale Netzwerke,
- Online-Werbung
- und mobile Plattformökosysteme.

Weniger stark adressiert werden hingegen digitale Arbeits- und Kollaborationsplattformen – obwohl gerade dort langfristige Lock-in-Effekte und hohe Wechselkosten entstehen.

Die wirtschaftliche Bedeutung moderner Office- und Kollaborationsökosysteme geht weit über klassische Softwareprodukte hinaus. Sie bilden zunehmend die operative Grundlage:

- öffentlicher Verwaltung,
- unternehmerischer Wissensarbeit,
- interner Kommunikation
- und organisatorischer Prozesse.

Dennoch existieren bislang nur eingeschränkte regulatorische Anforderungen hinsichtlich:

- interoperabler Dokumentformate,
- gleichwertiger Kommunikationsstandards,
- Workflow-Migration
- oder praktischer Austauschbarkeit zwischen Plattformökosystemen.

Der DMA adressiert damit zwar Plattformmacht im Konsumentenbereich, berücksichtigt jedoch die strukturelle Bedeutung digitaler Arbeitsökosysteme bislang nur begrenzt.

Cloud-Computing-Dienste und nummernunabhängige interpersonelle Kommunikationsdienste gehören zwar ausdrücklich zu den zentralen Plattformdiensten des DMA. Ein Cloud-Dienst wurde bis 2025 jedoch nicht benannt. Im November 2025 leitete die Kommission Marktuntersuchungen ein, ob AWS und Microsoft Azure trotz Unterschreitens der quantitativen Schwellenwerte als Gatekeeper zu benennen sind, sowie eine dritte Untersuchung, ob die Pflichten des DMA für Cloud-Märkte genügen — unter anderem bei Hindernissen für Interoperabilität.[30] Am 25. Juni 2026 teilte sie Amazon und Microsoft ihre vorläufige Auffassung mit, dass beide Dienste zu benennen sind; eine endgültige Entscheidung steht aus (Stand: November 2026).[31]

Diese Verfahren betreffen die Infrastrukturdienste AWS und Azure. Die darauf aufbauenden Büro- und Kollaborationsanwendungen, auf denen die tägliche Arbeit von Verwaltungen und Unternehmen beruht, erfassen sie nicht.

[30] Europäische Kommission: Eröffnung von drei Marktuntersuchungen zu Cloud-Computing-Diensten nach dem Digital Markets Act, 18. November 2025.

[31] Europäische Kommission: Commission reaches preliminary position that Amazon's and Microsoft's market leading cloud services should be designated under the DMA, 25. Juni 2026 (IP/26/1444).

6.3 Warum Arbeitsstandards kaum adressiert werden

Ein wesentlicher Grund dafür liegt in der historischen Entwicklung europäischer Plattformregulierung. Digitale Marktmacht wurde lange primär über:

- Suchmaschinen,
- soziale Netzwerke,
- E-Commerce
- und mobile Plattformen

definiert.

Dokumentenformate, Kollaborationsplattformen und digitale Arbeitsprozesse galten demgegenüber häufig als klassische Softwaremärkte – nicht als infrastrukturelle Machtstrukturen.

Tatsächlich haben sich moderne Kollaborationsplattformen jedoch längst zu zentralen digitalen Infrastrukturen entwickelt. Sie steuern:

- Kommunikation,
- Wissensorganisation,
- Identitätsmanagement,
- Dokumentflüsse
- und organisatorische Zusammenarbeit.

Gerade dadurch entstehen besonders starke Netzwerkeffekte. Unternehmen orientieren sich nicht nur an einzelnen Anwendungen, sondern zunehmend an kompletten Arbeitsökosystemen.

Die Frage interoperabler Arbeitsstandards wird dadurch zu einer zentralen wirtschafts- und wettbewerbspolitischen Herausforderung.

6.4 Plattformmacht im Büro statt im App Store

Die größte digitale Abhängigkeit europäischer Unternehmen entsteht heute häufig nicht im Bereich sozialer Medien oder mobiler App Stores, sondern innerhalb digitaler Arbeitsumgebungen.

Dokumente, Meetings, Chats, Kalender, Identität, Berechtigungen und Workflows werden zunehmend in integrierten Plattformökosystemen zusammengeführt. Dadurch verlagert sich Plattformmacht von einzelnen Anwendungen hin zu kompletten organisatorischen Arbeitswelten.

Die Wechselkosten solcher Systeme unterscheiden sich fundamental von klassischen Softwaremärkten. Unternehmen wechseln nicht mehr nur einzelne Programme, sondern potenziell:

- Kommunikationsstrukturen,
- Dokumentenlogiken,
- Prozesslandschaften,
- Identitätsmodelle
- und organisatorische Wissenssysteme.

Gerade dadurch entstehen neue Formen struktureller Plattformbindung, die sich nur eingeschränkt über klassische Wettbewerbsindikatoren erfassen lassen.

Die DMA-Gatekeeper-Frage bei Microsoft 365

Der Digital Markets Act definiert Gatekeeper anhand quantitativer Schwellenwerte wie Umsatz, Marktkapitalisierung und Nutzerzahlen; die Kommission kann Dienste nach einer Marktuntersuchung aber auch unterhalb dieser Schwellen benennen.

Microsoft-Dienste wie Teams oder Outlook erreichen erhebliche Reichweiten in europäischen Unternehmen und öffentlichen Einrichtungen. Microsoft meldete im Oktober 2023 mehr als 320 Millionen monatlich aktive Teams-Nutzer weltweit; neuere Zahlen hat das Unternehmen nicht veröffentlicht.[32]

Nach dem DMA ist Microsoft als Gatekeeper für das PC-Betriebssystem Windows und für LinkedIn benannt. Für den E-Mail-Dienst Outlook.com stellte die Kommission 2023 fest, dass Microsoft die quantitativen Schwellenwerte erreicht, benannte den Dienst aber nicht, weil Microsoft hinreichend begründet hatte, dass er kein wichtiges Zugangstor ist; 2024 schloss sie aus demselben Grund Bing, Edge und Microsoft Advertising aus.[33] Teams und die Office-Anwendungen sind keine benannten zentralen Plattformdienste.

Dadurch entsteht eine regulatorisch relevante Situation: Zentrale Bestandteile moderner Arbeitsökosysteme unterliegen bislang nur eingeschränkt spezifischen

[32] Microsoft, Ergebnisse für das erste Quartal des Geschäftsjahrs 2024 (Earnings Call), 24. Oktober 2023.
[33] Europäische Kommission, Benennungsbeschluss vom 5. September 2023 (Microsoft); Beschluss C(2024) 806 vom 12. Februar 2024, Zusammenfassung in ABl. C/2024/2709.

Interoperabilitätsverpflichtungen des DMA – obwohl gerade dort erhebliche strukturelle Wechselkosten und Plattformabhängigkeiten entstehen.

Bemerkenswert ist, dass die Kommission die Interoperabilität von Kollaborationswerkzeugen nicht über den DMA, sondern im Kartellverfahren adressiert hat. Am 12. September 2025 erklärte sie Zusagen Microsofts für verbindlich: Microsoft bietet Office- und Microsoft-365-Pakete ohne Teams an, gewährleistet die Interoperabilität zentraler Funktionen zwischen konkurrierenden Kollaborationswerkzeugen und bestimmten Microsoft-Produkten und ermöglicht den Export von Teams-Nachrichtendaten. Die Zusagen zu Interoperabilität und Datenportabilität gelten zehn Jahre; ein Treuhänder überwacht die Umsetzung.[34]

Das zeigt zweierlei. Die Kommission erkennt asymmetrische Interoperabilität in digitalen Arbeitsumgebungen als Wettbewerbsproblem an. Zugleich bleibt die Lösung eine Einzelfallregelung für ein Unternehmen und ein Produkt, deren Wirksamkeit Dritte nicht anhand offener, reproduzierbarer Tests überprüfen können.

Die eigentliche Marktmacht moderner Plattformen entsteht zunehmend über:

- Integrationstiefe,
- Workflow-Abhängigkeit,
- Identitätsmanagement,
- API-Kontrolle
- und asymmetrische Interoperabilität.

Genau dieser Bereich bleibt vom DMA in seiner aktuellen Form bislang nur teilweise erfasst.

6.5 Fehlende regulatorische Interoperabilitätsmechanismen

Der DMA enthält zwar einzelne Interoperabilitätsanforderungen, adressiert jedoch bislang kaum die Frage überprüfbarer praktischer Interoperabilität komplexer Arbeits- und Kollaborationssysteme.

Insbesondere fehlen bislang:

[34] Europäische Kommission: Commission accepts commitments offered by Microsoft to address competition concerns related to Teams, Pressemitteilung vom 12. September 2025, Sachen AT.40721 und AT.40873.

- standardisierte Compliance-Tests,
- interoperable Referenzimplementierungen,
- regulatorische Konformitätsprüfungen
- sowie verbindliche Kriterien praktischer Austauschbarkeit.

Dadurch entsteht eine regulatorische Lücke:
Standards können formal existieren, ohne dass ihre tatsächliche interoperable Umsetzung überprüft wird.

Gerade in hoch konzentrierten Plattformmärkten reicht formale Offenheit jedoch nicht aus. Ohne überprüfbare Konformität entstehen weiterhin:

- strukturelle Lock-in-Effekte,
- hohe Wechselkosten
- und langfristige Marktasymmetrien.

Die zentrale Herausforderung digitaler Souveränität besteht daher nicht ausschließlich in der Existenz offener Standards, sondern zunehmend in ihrer praktischen Durchsetzbarkeit.

Der DMA hat begonnen, digitale Plattformmacht regulatorisch zu adressieren. Die Frage überprüfbarer Interoperabilität digitaler Arbeitsökosysteme bleibt jedoch bislang weitgehend ungelöst.

6.6 European Interoperability Framework und Interoperable Europe Act

Die Europäische Union verfügt mit dem European Interoperability Framework (EIF) bereits über einen wichtigen strategischen Rahmen zur Förderung interoperabler digitaler Verwaltungssysteme. Das EIF definiert grundlegende Prinzipien organisatorischer, semantischer, technischer und rechtlicher Interoperabilität innerhalb europäischer Verwaltungsstrukturen.

Damit erkennt die Europäische Union die strategische Bedeutung interoperabler digitaler Systeme grundsätzlich bereits an. Das EIF adressiert insbesondere:

- offene Standards,
- Wiederverwendbarkeit,
- grenzüberschreitende Zusammenarbeit
- sowie langfristige digitale Nachhaltigkeit.

Das Framework besitzt jedoch primär empfehlenden und konzeptionellen Charakter. Verbindliche technische Konformitätsprüfungen, interoperable Referenzimplementierungen oder standardisierte Compliance-Mechanismen komplexer Plattformökosysteme stehen bislang weniger im Mittelpunkt.

Mit dem Interoperable Europe Act ist 2024 ein verbindlicher Rechtsrahmen hinzugekommen. Öffentliche Stellen müssen seit 12. Januar 2025 eine Interoperabilitätsbewertung durchführen, bevor sie verbindliche Anforderungen an transeuropäische digitale öffentliche Dienste festlegen oder wesentlich ändern; ein Interoperable Europe Board koordiniert die Umsetzung.[35] Der Rechtsakt zielt auf die grenzüberschreitende Interoperabilität öffentlicher Dienste. Ob die Büro- und Kollaborationsplattformen, mit denen Verwaltungen arbeiten, praktisch austauschbar sind, prüft er nicht.

Gerade moderne Kollaborations- und Wissensplattformen erzeugen heute jedoch strukturelle Abhängigkeiten, die weit über klassische Verwaltungsinteroperabilität hinausgehen. Die praktische Wechselbarkeit integrierter Arbeitsumgebungen hängt zunehmend von organisatorischen Workflows, Plattform-APIs, semantischen Modellen und KI-gestützten Kontextsystemen ab.

Das EIF bildet damit einen wichtigen strategischen Ausgangspunkt europäischer Interoperabilitätspolitik. Die Frage überprüfbarer praktischer Interoperabilität komplexer Plattformökosysteme bleibt jedoch bislang nur eingeschränkt adressiert.

[35] Verordnung (EU) 2024/903 (Interoperable Europe Act), ABl. L vom 22. März 2024, insb. Art. 3; Interoperable Europe Portal: Interoperability assessments are now mandatory, 13. Januar 2025.

6.7 Der Data Act: wichtiger Fortschritt – aber keine ausreichende Antwort auf moderne Plattformbindung

Mit dem Data Act hat die Europäische Union einen wichtigen regulatorischen Schritt gesetzt, um strukturelle Abhängigkeiten in digitalen Märkten zu reduzieren. Der Data Act adressiert insbesondere Datenportabilität, Cloud Switching und technische Wechselbarrieren zwischen digitalen Diensten. Anbieter sollen Wechsel nicht künstlich erschweren, überhöhte Exit-Kosten vermeiden und standardisierte Schnittstellen für Datenmigration bereitstellen.

Der Data Act gilt seit 12. September 2025; Entgelte für den Anbieterwechsel sind ab 12. Januar 2027 untersagt. Aufschlussreich ist die Abstufung der technischen Pflichten: Nur Anbieter von Infrastrukturdiensten (IaaS) müssen ihre Kunden dabei unterstützen, beim neuen Anbieter funktionale Gleichwertigkeit zu erreichen. Anbieter von Plattform- und Softwarediensten — also auch von Büro- und Kollaborationsplattformen — müssen offene Schnittstellen bereitstellen und, solange keine gemeinsamen Spezifikationen veröffentlicht sind, Daten in einem strukturierten, gängigen und maschinenlesbaren Format exportieren.[36] Sobald gemeinsame Spezifikationen oder harmonisierte Normen für die Interoperabilität solcher Dienste im zentralen Unionsverzeichnis veröffentlicht sind, müssen die Dienste zudem mit ihnen kompatibel sein (Art. 30 Abs. 3, Art. 35). Bis dahin verlangt der Data Act gerade für die Dienste, um die es in diesem Papier geht, den Export der Daten, nicht die Gleichwertigkeit der Funktion. Offen ist, ob künftige Spezifikationen die praktische Wechselbarkeit komplexer Arbeitsumgebungen erfassen werden — mit Arbeitsabläufen, Berechtigungen und organisatorischem Kontext.

Gerade im Bereich von Cloud-Infrastruktur und Plattformdiensten stellt dies einen wichtigen Fortschritt dar. Die Maßnahmen sind wirtschaftspolitisch sinnvoll und notwendig. Sie adressieren jedoch primär infrastrukturelle und datenbezogene Abhängigkeiten. Die tatsächliche Wechselbarkeit moderner digitaler Arbeitsökosysteme geht heute weit darüber hinaus.

Die strukturelle Plattformbindung moderner Kollaborations- und Wissenssysteme entsteht zunehmend nicht allein über Datenbestände, sondern über integrierte Workflows, organisatorische Prozesslogiken, Berechtigungsmodelle, Automatisierungsmechanismen, plattformspezifische APIs und semantische

[36] Verordnung (EU) 2023/2854 (Data Act), Art. 2 Nr. 37, Art. 29 und Art. 30.

Verknüpfungen zwischen unterschiedlichen Diensten. Mit dem Übergang zu KI-gestützten Arbeitsumgebungen verstärkt sich diese Entwicklung zusätzlich.

Ein Export von Dateien oder Daten garantiert daher noch keine reale organisatorische Wechselbarkeit.

Besonders deutlich wird dies bei modernen Arbeitsplatz- und Kollaborationsplattformen. Unternehmen integrieren heute Dokumentenmanagement, Kommunikation, Meetings, Aufgabenverwaltung, Identitätsmanagement und Workflow-Automatisierung zunehmend in gemeinsame Plattformökosysteme. Dadurch entstehen erhebliche Produktivitäts- und Integrationsvorteile. Gleichzeitig steigen jedoch auch die organisatorischen Wechselkosten.

Die eigentliche Herausforderung liegt häufig nicht mehr in der Migration einzelner Datenbestände, sondern in der Wiederherstellung funktionaler organisatorischer Abläufe innerhalb alternativer Systeme. Dokumente können exportiert werden, ohne dass dadurch automatisch Automatisierungsprozesse, Freigabeworkflows, Integrationen, Berechtigungslogiken oder organisatorisches Kontextwissen verlustfrei migriert werden können.

Die nächste Phase digitaler Plattformabhängigkeit entsteht damit zunehmend auf semantischer und organisatorischer Ebene – nicht ausschließlich auf Ebene von Daten oder Infrastruktur.

Der Data Act adressiert diese Problematik bislang nur eingeschränkt; der von der Kommission vorgeschlagene Digital Omnibus sieht für bestimmte Dienste, die keine Infrastrukturdienste sind, sogar Erleichterungen vor.[37] Datenportabilität bleibt eine notwendige Voraussetzung digitaler Souveränität, sie ist jedoch keine hinreichende Bedingung für reale Wechselbarkeit komplexer Arbeits- und Wissensplattformen.

Gerade deshalb gewinnt die Frage überprüfbarer praktischer Interoperabilität weiter an Bedeutung. Digitale Souveränität bedeutet künftig nicht nur die Fähigkeit, Daten zu exportieren, sondern zunehmend auch die Fähigkeit, organisatorische Arbeitsprozesse, semantische Wissensstrukturen und digitale

[37] Vorschlag der Europäischen Kommission für einen Digital Omnibus, November 2025.

Zusammenarbeit plattformübergreifend interoperabel und migrationsfähig zu halten.

6.8 Der Cloud and AI Development Act (CADA)

Mit dem Vorschlag für einen Cloud and AI Development Act vom 3. Juni 2026 schlägt die Kommission erstmals Souveränitätsstufen für Cloud-Dienste vor.[38] Bei der Wechselfähigkeit stützt sich der Vorschlag auf die Bestimmungen des Data Act; auf den höheren Stufen verlangt er dokumentierte Migrationspläne. Eine erprobte Ausstiegsfähigkeit der öffentlichen Stelle macht er jedoch nicht zur allgemeinen Anforderung, und praktische Interoperabilität wird nicht geprüft.[39]

Der Policy Brief Nr. 2026-001 schlägt deshalb vor, auf jeder CADA-Stufe dokumentierte Datenportabilität, offene Formate und einen erprobten Ausstiegsplan zu verlangen und die Stufen mittelfristig an eine europäische Interoperabilitätszertifizierung zu koppeln. Kapitel 9 dieses Papiers entwickelt diese Zertifizierung.

[38] Vorschlag für eine Verordnung zur Stärkung des europäischen Cloud- und KI-Ökosystems (Cloud and AI Development Act), COM(2026) 502 final vom 3. Juni 2026.

[39] Zur Analyse siehe Illsinger, W. (2026): Digitale Souveränität in Europa. Definition, Status, Handlungsoptionen. Policy Brief Nr. 2026-001, Version 3. Wien: 4future.institute. DOI: 10.5281/zenodo.24042085. Abschnitt 2.4.

7 Die nächste Lock-in-Welle: KI und semantische Plattformen

Die folgenden Beobachtungen beschreiben sich abzeichnende Entwicklungen auf Basis aktueller Markttrends. Sie erheben keinen Anspruch auf Vollständigkeit, sondern sollen auf strukturelle Risiken hinweisen, die heute bereits erkennbar sind.

Die Diskussion über digitale Souveränität konzentriert sich heute noch stark auf Infrastruktur:

- Rechenzentren,
- Cloud-Plattformen,
- Netzwerke
- und Datenlokation.

Diese Perspektive greift jedoch zunehmend zu kurz. Digitale Abhängigkeit verschiebt sich schrittweise von der reinen Infrastruktur hin zu integrierten Wissens-, Kontext- und KI-Systemen.

Abbildung 2 verdeutlicht diese Entwicklung anhand dreier Ebenen technologischer Souveränität:

1. digitale Infrastruktur,
2. Interaktion mit der physischen Welt,
3. Daten und Wissen.

Während die erste Phase digitaler Souveränität primär Infrastrukturfragen betraf, entstehen die strategisch relevantesten Abhängigkeiten künftig zunehmend auf Ebene semantischer Wissens- und KI-Systeme.



Abbildung 2: Ebenen digitaler Souveränität und technologischer Abhängigkeit

Die Bedeutung interoperabler Standards wächst damit erheblich. Dokumente, Kommunikationssysteme, Plattformen und APIs bilden nicht mehr nur technische Arbeitswerkzeuge, sondern zunehmend die semantische Grundlage KI-gestützter Systeme.

7.1 Von Dokumenten zu Wissensmodellen

Die nächste Phase digitaler Plattformabhängigkeit entsteht nicht mehr primär auf Ebene einzelner Dokumente oder Anwendungen, sondern auf Ebene semantischer Wissensmodelle und KI-gestützter Arbeitsprozesse.

Während frühere Lock-in-Effekte vor allem durch proprietäre Dateiformate oder Plattformintegrationen entstanden, verlagert sich digitale Abhängigkeit zunehmend auf:

- Wissensstrukturen,
- Kontextmodelle,
- semantische Verknüpfungen,
- KI-gestützte Automatisierung
- und plattformgebundene Datenräume.

Moderne Dokumentformate sind dabei längst mehr als reine Dateiformate. Sie bilden die infrastrukturelle Grundlage digitaler Wissensarbeit und entwickeln sich zunehmend zu semantischen Trägern organisatorischen Wissens.

Dokumente enthalten heute nicht nur Inhalte, sondern auch:

- Kommentare,
- Metadaten,
- Versionshistorien,
- Freigaben,
- Kollaborationsinformationen
- und organisatorische Kontextstrukturen.

KI-Systeme greifen genau auf diese Strukturen zu. Inhalte werden nicht mehr nur gespeichert oder ausgetauscht, sondern durch KI-Systeme:

- interpretiert,
- priorisiert,
- verknüpft
- und automatisiert verarbeitet.

Dadurch entsteht eine neue Form digitaler Abhängigkeit:
Nicht mehr allein der Zugriff auf Daten entscheidet über Wechselbarkeit, sondern die Kontrolle über deren semantische Interpretation.

7.2 Proprietäre KI-Ökosysteme

Moderne KI-Systeme entwickeln ihre Stärke zunehmend durch tiefe Integration in bestehende Plattformökosysteme. KI-Assistenten greifen auf:

- Dokumente,
- Kommunikation,
- Kalender,
- Meetings,
- Berechtigungen,
- Wissensdatenbanken
- und organisatorische Prozesse

zu und verbinden diese Informationen zu kontextbezogenen Arbeitsmodellen.[40]

Der eigentliche Wert solcher Systeme entsteht dadurch weniger durch einzelne KI-Modelle als durch den exklusiven Zugriff auf integrierte Daten- und Workflow-Ökosysteme.

[40] Cortiñas-Lorenzo, Karina et al., „Through the Looking-Glass: Transparency Implications and Challenges in Enterprise AI Knowledge Systems", arXiv:2401.09410, Januar 2024"

Je stärker KI-Funktionen mit proprietären Plattformen verbunden werden, desto schwieriger wird die Migration organisatorischen Wissens in alternative Systeme. Digitale Abhängigkeit entsteht dadurch zunehmend nicht nur über Datenformate, sondern über:

- Kontextwissen,
- semantische Verknüpfungen
- und plattformgebundene Wissensmodelle.

Die Kontrolle über KI-Ökosysteme entwickelt sich damit zu einer neuen Form infrastruktureller Marktmacht.

7.3 KI-Agenten und semantische Abhängigkeiten

Mit der Entwicklung autonomer KI-Agenten verschärft sich diese Problematik zusätzlich. KI-Agenten interagieren nicht mehr nur mit einzelnen Dokumenten, sondern zunehmend mit:

- Arbeitsabläufen,
- Kommunikationssystemen,
- Unternehmenswissen
- und organisatorischen Prozessen.

Dadurch entstehen neue Formen semantischer Lock-in-Effekte. Arbeitslogiken, Priorisierungen, Kontextmodelle und organisatorische Wissensstrukturen werden schrittweise in proprietären KI-Systemen abgebildet.

Die Migration solcher Systeme wird erheblich komplexer als klassische Datenmigration. Selbst wenn Daten exportierbar bleiben, bedeutet dies nicht automatisch, dass:

- Kontextwissen,
- Automatisierungen,
- semantische Beziehungen
- oder organisatorische Arbeitslogiken

gleichwertig migriert werden können.

Konkret geht es unter anderem um die Berechtigungen, auf die ein Assistent zugreifen darf, um Verknüpfungen zwischen Antworten und Quellen, um Wissensgraphen, um die Konfiguration von Agenten und um den Zustand

laufender Prozesse. Für einzelne Bestandteile gibt es offene Standards — für Wissensgraphen etwa die W3C-Standards RDF und JSON-LD. Für die Übertragung eines integrierten KI-Arbeitskontexts als Ganzes, mit Berechtigungen, Quellenbezügen, Agentenkonfiguration und Prozesszustand, gibt es jedoch kein etabliertes offenes Format.

Die eigentliche Plattformabhängigkeit entsteht damit zunehmend auf Ebene:

- semantischer Modelle,
- organisatorischer Wissensstrukturen
- und KI-gestützter Entscheidungslogiken.

7.4 APIs als neue Standards

APIs („Application Programming Interfaces") entwickeln sich im KI-Zeitalter zunehmend zu den eigentlichen Standards digitaler Plattformökosysteme. Sie definieren[41]:

- wie KI-Systeme auf Daten zugreifen,
- wie Anwendungen integriert werden,
- wie Automatisierungen funktionieren
- und welche Plattformdienste miteinander interagieren können.

Formal offene APIs reichen dabei zunehmend nicht mehr aus, um reale Wechselbarkeit sicherzustellen. Proprietäre Erweiterungen, plattformspezifische SDKs, semantische Modelle und nicht standardisierte Integrationen erzeugen neue Abhängigkeiten, die weit über klassische Dateiformate hinausgehen.

Besonders relevant wird dies bei:

- KI-Agenten,
- Workflow-Automatisierung,
- Wissensgraphen,
- semantischen Suchsystemen
- und plattformintegrierten KI-Assistenten.

[41] Sharma, Rishi et al., „Collaborative Agentic AI Needs Interoperability Across Ecosystems", arXiv:2505.21550, Mai 2025"

Wer die APIs kontrolliert, kontrolliert zunehmend auch die semantische Infrastruktur digitaler Arbeit.

7.5 Risiken für europäische digitale Souveränität

Die nächste Phase digitaler Souveränität wird daher nicht allein über:

- Cloud-Infrastruktur,
- Rechenzentren
- oder Datenlokation

entschieden.

Entscheidend wird zunehmend die Frage, ob:

- Wissensmodelle,
- KI-gestützte Arbeitsprozesse,
- semantische Integrationen
- und organisatorische Kontextsysteme

langfristig interoperabel und migrierbar bleiben.

Fehlende Interoperabilität im KI-Bereich birgt erhebliche Risiken:

- steigende organisatorische Abhängigkeiten,
- langfristige Plattformbindung,
- eingeschränkte Wechselbarkeit
- und neue Konzentrationseffekte in digitalen Märkten.

Gerade deshalb gewinnt die Frage überprüfbarer Interoperabilität weiter an Bedeutung. Die Herausforderungen, die bereits heute bei Dokumentformaten, APIs und Kollaborationsplattformen sichtbar werden, drohen sich im Bereich KI und semantischer Plattformen deutlich zu verstärken.

Digitale Souveränität bedeutet unter diesen Bedingungen nicht nur Kontrolle über Daten, sondern zunehmend auch Kontrolle über:

- semantische Strukturen,
- organisatorisches Wissen
- und KI-gestützte Arbeitsprozesse.

8 Warum offene Standards allein nicht ausreichen

Die vorangegangenen Kapitel haben anhand konkreter Beispiele gezeigt, dass formale Standardisierung keine hinreichende Bedingung für praktische Interoperabilität ist. Dieses Kapitel fasst die strukturellen Muster zusammen.

8.1 Das Problem rein formaler Standardisierung

OOXML ist seit 2008 ISO-Standard. Microsoft Office unterstützte die bereinigte Strict-Variante zunächst nicht und speichert bis heute standardmäßig im Übergangsformat Transitional, das für neue Dokumente nicht gedacht war (siehe Abschnitt 3.3). CalDAV (2007) und CardDAV (2011) sind seit vielen Jahren IETF-Standards; Outlook unterstützt sie bis heute nicht nativ (siehe Abschnitt 4.3). IMAP wurde 1988 erstmals spezifiziert; im neuen Outlook bleibt es gegenüber Exchange-Konten funktional eingeschränkt (siehe Abschnitt 4.2).

Das Muster ist konsistent: Formale Standardisierung garantiert keine reale Austauschbarkeit. Standards entfalten ihre marktwirtschaftliche Wirkung nur dann, wenn ihre Implementierung konsistent erfolgt und interoperables Verhalten überprüfbar bleibt.

8.2 Fehlende Compliance-Prüfung

Exchange Web Services war eine dokumentierte Schnittstelle, auf der Drittanbieter jahrelang aufgebaut haben. Seit Oktober 2026 wird sie schrittweise deaktiviert, ab April 2027 endgültig abgeschaltet; der Nachfolger Microsoft Graph ist eine proprietäre API ohne standardisierte Alternative (siehe Abschnitt 4.4). Ob dieser Wechsel die Interoperabilität für Dritte wahrt, ließe sich nach geltendem Recht allenfalls im Einzelfall klären, etwa in einem kartellrechtlichen Verfahren. Eine vorab festgelegte, öffentlich nachvollziehbare Prüfung solcher Schnittstellenwechsel gibt es nicht: Die besonderen Interoperabilitätspflichten des DMA greifen nicht, weil Microsoft 365 kein benannter zentraler Plattformdienst ist (siehe Abschnitt 6.4), und die Teams-Zusagen von 2025 sind eine Einzelfallregelung, deren Umsetzung ein Treuhänder überwacht — kein allgemeiner, öffentlich überprüfbarer Maßstab.

Compliance-Prüfung fehlt nicht nur technisch – sie fehlt regulatorisch.

8.3 Fehlende Referenzimplementierungen

OOXML Strict existiert als Spezifikation. Eine verbindliche Referenzimplementierung, die zeigt wie Strict korrekt implementiert wird – existiert nicht. Das Ergebnis: Dominante Marktimplementierungen definieren faktisch den Standard *(siehe Kapitel 0)*. Dasselbe gilt für S3-kompatible Speicherdienste – "kompatibel" ohne Referenzmaßstab ist bedeutungslos *(siehe Kapitel 4.5)*.

8.4 Fehlende Migrationsfähigkeit

Interoperabilität wird häufig auf Datenexport reduziert. Tatsächliche Wechselbarkeit umfasst jedoch Workflows, Berechtigungen, Metadaten, Kommunikationshistorien und organisatorische Kontextinformationen *(siehe Kapitel 5.3, 5.4, 5.5)*. Gerade bei KI-gestützten Systemen entsteht die nächste Generation von Abhängigkeiten auf semantischer Ebene – nicht auf Dateiebene *(siehe Kapitel 7)*.

8.5 „Open Washing" und Scheinkompatibilität

Die dokumentierten Beispiele zeigen ein einheitliches Muster: Plattformen werben mit Offenheit – OOXML als "offener Standard", EWS als "dokumentierte Schnittstelle", S3 als "kompatibles Protokoll" – ohne dass daraus gleichwertige Nutzbarkeit oder reale Wechselbarkeit folgt.

Das ist nicht zwingend das Ergebnis böser Absicht, und die Kritik dieses Papiers setzt eine solche Absicht auch nicht voraus. Sie richtet sich gegen den nachweisbaren Mechanismus: Ein Markt ohne überprüfbare Konformitätsmechanismen verschiebt die Kosten der Abweichung auf alternative Anbieter und auf Kunden, die wechseln wollen.

Standards ohne überprüfbare Konformität sind keine Standards. Sie sind Versprechen.

8.6 Unterschiedliche Probleme, unterschiedliche Antworten

Die Beispiele dieses Papiers beschreiben verwandte, aber unterschiedliche Probleme, die unterschiedliche Antworten erfordern:

- **Dokumentformate:** die zuverlässige Verarbeitung standardisierter Inhalte zwischen unabhängigen Implementierungen;
- **CalDAV und CardDAV:** die Unterstützung erforderlicher offener Schnittstellen überhaupt;
- **IMAP:** die Abgrenzung zwischen E-Mail-Funktionen, die der Standard abdeckt, und Kalenderfunktionen, für die andere offene Standards bestehen;
- **EWS und Microsoft Graph:** die Kontrolle über den Lebenszyklus von Schnittstellen und die Anpassungskosten Dritter;
- **Arbeitsabläufe:** die Übertragbarkeit organisatorischer Abläufe, Berechtigungen und Kontextinformationen.

Ein Produkt kann ein unterstütztes Protokoll korrekt implementieren und zugleich wichtige offene Schnittstellen gar nicht anbieten. Eine reine Konformitätsprüfung wäre deshalb zu wenig. Erforderlich sind beides: verbindliche Mindestanforderungen, welche offenen Schnittstellen ein Dienst unterstützen muss, und Prüfungen, ob er sie zuverlässig umsetzt.

9 Vorschlag: Europäische Interoperabilitäts-Zertifizierung

9.1 Grundidee und Zielsetzung

Die bisherigen Kapitel zeigen ein strukturelles Problem digitaler Märkte: Offene Standards allein reichen nicht aus, um reale Austauschbarkeit und funktionierenden Wettbewerb sicherzustellen. Entscheidend ist nicht nur die Existenz eines Standards, sondern dessen überprüfbare interoperable Umsetzung.

Genau hier setzt der Vorschlag einer europäischen Interoperabilitäts-Zertifizierung an.

Ziel eines solchen Systems wäre es nicht, technologische Innovation zu regulieren, einzelne Plattformen zu benachteiligen — oder technologische Autarkie herzustellen. Ziel wäre vielmehr die Schaffung überprüfbarer Markttransparenz:

- Welche Systeme implementieren Standards tatsächlich interoperabel?
- Welche Plattformen ermöglichen reale Wechselbarkeit?
- Welche Lösungen erzeugen langfristige strukturelle Abhängigkeiten?

Eine europäische Interoperabilitäts-Zertifizierung würde damit eine ähnliche Funktion erfüllen wie technische Zertifizierungen in klassischen Industrien:
Sie würde nicht Innovation verhindern, sondern Vertrauen, Austauschbarkeit und Markttransparenz schaffen.

9.2 Unabhängige europäische Zertifizierungsstelle

Voraussetzung für ein glaubwürdiges Interoperabilitäts-Zertifizierungssystem wäre ein unabhängiger europäischer Governance- und Prüfrahmen.

Die Aufgabe einer solchen Struktur bestünde nicht darin, einzelne Technologien oder Anbieter zu bevorzugen, sondern die objektive Überprüfung praktischer Interoperabilität auf Basis transparenter technischer Kriterien sicherzustellen.

Ein geeignetes Modell wäre ein dezentrales Netzwerk national akkreditierter Prüfstellen unter einem gemeinsamen europäischen Rahmenwerk – vergleichbar mit bestehenden Konformitäts- und Zertifizierungssystemen in anderen Industriebereichen.

Europa verfügt bereits über zahlreiche institutionelle Strukturen, die hierfür als organisatorische Grundlage dienen könnten. Dazu zählen insbesondere:

- nationale Normungs- und Zertifizierungsorganisationen wie Austrian Standards (Österreich), DIN (Deutschland), AFNOR (Frankreich),
- europäische Normungsorganisationen wie CEN, CENELEC und ETSI,
- spezialisierte Behörden wie ENISA im Bereich europäischer Cybersicherheitszertifizierung
- sowie bestehende nationale IT-Zertifizierungsstellen wie das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI).

Dadurch müsste kein vollständig neues institutionelles System geschaffen werden. Vielmehr könnte ein interoperabler europäischer Zertifizierungsrahmen auf bestehenden Normungs-, Prüf- und Akkreditierungsstrukturen aufbauen.

Entscheidend wäre dabei institutionelle Unabhängigkeit:
Die Zertifizierung müsste:

- transparent,
- nachvollziehbar,
- reproduzierbar
- und herstellerneutral

erfolgen.

Nur dadurch kann das notwendige Vertrauen entstehen – bei Unternehmen, öffentlichen Institutionen und alternativen Anbietern gleichermaßen.

9.3 Technische Compliance-Tests

Kernbestandteil einer Interoperabilitäts-Zertifizierung wären standardisierte technische Compliance-Tests.

Dabei ginge es nicht nur um die Frage, ob ein Standard formal implementiert wurde, sondern ob unterschiedliche Systeme praktisch interoperabel funktionieren.

Solche Tests könnten beispielsweise prüfen:

- konsistente Dokumentdarstellung,
- verlustfreie Migration,
- interoperable Kalender- und Kontaktsynchronisation,
- API-Kompatibilität,
- Workflow-Verhalten,
- Berechtigungsmodelle
- oder plattformübergreifende Kollaborationsfunktionen.

Besonders relevant wäre dabei die praktische Nutzerperspektive: Interoperabilität muss sich nicht nur theoretisch, sondern im realen Einsatz bewähren.

Gerade in komplexen Plattformökosystemen reicht reine Spezifikationskonformität häufig nicht aus, um reale Austauschbarkeit sicherzustellen.

9.4 Referenzimplementierungen und Test-Suites

Technische Standards benötigen überprüfbare Referenzmodelle. Daher sollte eine europäische Interoperabilitäts-Zertifizierung durch:

- offene Referenzimplementierungen,
- standardisierte Test-Suites
- und öffentlich dokumentierte Konformitätskriterien

ergänzt werden.

Ziel wäre die Reduktion interpretativer Spielräume und asymmetrischer Implementierungen.

Grundlage sollte ein öffentlich zugängliches Testkorpus sein. Jeder Testfall sollte mindestens dokumentieren:

- **Ausgangsdokument:** verwendete Funktion und beanspruchtes Formatprofil;
- **Testumgebung:** Produkte, Versionen und relevante Einstellungen;
- **erwartetes Verhalten:** die Grundlage in der Spezifikation oder im Prüfprofil;
- **tatsächliches Verhalten:** die reproduzierbare Abweichung;
- **Bearbeitungszyklus:** nicht nur das Öffnen, sondern auch Bearbeiten und Speichern im alternativen Produkt und das erneute Öffnen im Ausgangsprodukt;
- **Einordnung:** Normverletzung, Lücke in der Spezifikation, Herstellererweiterung oder Implementierungsfehler;
- **Folge für den Kunden:** Informationsverlust, Nachbearbeitung oder Wechselhindernis.

Einflussfaktoren wie fehlende Schriftarten sind dabei zu kontrollieren; nicht jeder Layoutfehler ist eine Normverletzung. Gerade diese Sorgfalt macht die Befunde belastbar: Strukturelle Probleme lassen sich dann nicht als bloße Fehler konkurrierender Programme abtun, und die Einordnung zeigt, ob die Implementierung korrigiert, die Norm präzisiert oder ein Interoperabilitätsprofil ergänzt werden muss.

Gerade im Bereich:

- von Dokumentformaten,
- APIs,
- Kollaborationsplattformen
- und KI-gestützten Workflow-Systemen

könnten solche Referenzmodelle erheblich zur praktischen Interoperabilität beitragen.

Die Referenzimplementierung selbst würde weder zum verpflichtenden Marktstandard noch zum unangreifbaren Maßstab. Maßgeblich bleiben die veröffentlichten Anforderungen; die Referenzimplementierung ist ein Hilfsmittel, um sie zu prüfen.

Dadurch ließe sich die heute häufig bestehende Situation vermeiden, in der dominante Marktimplementierungen faktisch selbst zum Referenzstandard werden.

9.5 Zertifizierungsstufen, Durchsetzung und Finanzierung

Nicht jede Form von Interoperabilität besitzt denselben Reifegrad. Daher erscheint ein gestuftes Zertifizierungsmodell sinnvoll. Ein Zertifikat sollte dabei nicht pauschal „Interoperabilität" zusichern, sondern die Erfüllung eines verbindlichen, versionierten Prüfprofils mit definierten Funktionen, zulässigen Toleranzen und klaren Bestehenskriterien. Innerhalb eines Profils muss der Anspruch streng bleiben: Eine wesentliche Inkompatibilität lässt sich nicht durch überwiegend vorhandene Konformität aufwiegen. Um Verwechslungen mit den Souveränitätsstufen 1 bis 4 des CADA zu vermeiden, werden die Zertifizierungsstufen hier mit römischen Ziffern bezeichnet.

Stufe I – Geprüftes Basisprofil

Unabhängig geprüft ist, dass der Dienst ein verbindliches Basisprofil einhält — die offenen Standards und Grundfunktionen, die für den jeweiligen Diensttyp mindestens erforderlich sind. Der Anbieter dokumentiert zudem Abweichungen und herstellerspezifische Erweiterungen. Diese Offenlegung ist Pflicht, legitimiert aber keine Verletzung des Basisprofils: Wer das Basisprofil nicht erfüllt, erhält das Zertifikat nicht, auch wenn er die Abweichung offenlegt.

Dies garantiert noch keine vollständige praktische Austauschbarkeit, schafft jedoch Markttransparenz als Grundlage informierter Beschaffungs- und Architekturentscheidungen.

Stufe II – Geprüfte Interoperabilität

Für die Funktionen eines versionierten Prüfprofils ist in Tests mit unabhängigen Implementierungen nachgewiesen, dass sie innerhalb der festgelegten Toleranzen übereinstimmend verarbeitet werden.

Prüfprofile können etwa Dokumentdarstellung, Kalender- und Kontaktsynchronisation, Metadaten, Kommentare und Versionen oder plattformübergreifende Zusammenarbeit umfassen.

Stufe III – Geprüfte Wechselfähigkeit

Die höchste Stufe bestätigt in einem standardisierten Referenzszenario, dass Daten, Dokumente, Metadaten, Berechtigungen und definierte Arbeitsabläufe zu einer unabhängigen Implementierung migriert werden können. Der Nachweis dokumentiert neben dem erhaltenen Funktionsumfang auch Arbeitsaufwand,

Kosten, Dauer von Parallelbetrieb und Betriebsunterbrechung sowie verbleibende Abhängigkeiten.

Eine technisch mögliche Migration ist keine ausreichende Wechseloption, wenn sie unverhältnismäßige Kosten, monatelangen Parallelbetrieb oder umfangreiche manuelle Rekonstruktion erfordert. Das ist keine Forderung nach einem kostenlosen oder aufwandslosen Anbieterwechsel, sondern die notwendige Unterscheidung zwischen theoretischer Exportierbarkeit und einer tatsächlich ausführbaren Handlungsoption.

Für alle Stufen gilt:

- Prüfkriterien und Ergebnisse sind öffentlich zugänglich;
- bei relevanten Produktänderungen wird erneut geprüft;
- festgestellte Mängel sind innerhalb einer Frist zu beheben;
- bei Nichterfüllung wird das Zertifikat ausgesetzt oder entzogen.

Durchsetzung und wirtschaftliche Relevanz

Zertifizierungsstufen entfalten ihre Wirkung nur dann, wenn sie wirtschaftlich und regulatorisch relevant werden.

Dafür erscheinen insbesondere vier Mechanismen geeignet:

Öffentliche Beschaffung: Vergabeverfahren öffentlicher Institutionen könnten schrittweise interoperabilitätsbezogene Mindestanforderungen definieren. So könnte beispielsweise für allgemeine Arbeitsplatzsysteme mindestens Stufe I, für langfristig archivierungspflichtige oder besonders kritische Systeme mindestens Stufe II vorgesehen werden. Das entspricht dem etablierten Prinzip technischer Konformitätsnachweise in anderen Industriebereichen: Nicht der Anbieter wird reguliert, sondern die interoperable Eigenschaft des Produkts wird transparent nachgewiesen.

Integration in bestehende DMA-Interoperabilitätsmechanismen: Für besonders marktmächtige Plattformanbieter könnten Interoperabilitätszertifizierungen perspektivisch stärker mit bestehenden regulatorischen Instrumenten – etwa im Umfeld des Digital Markets Act – verknüpft werden. Dies würde insbesondere dort relevant, wo Plattformökosysteme erhebliche Wechselkosten erzeugen, organisatorische Abhängigkeiten entstehen oder asymmetrische Interoperabilität strukturelle Marktvorteile schafft.

Transparenzpflicht: Anbieter digitaler Arbeitsplatz-, Kollaborations- und Plattformlösungen könnten verpflichtet werden, ihren Interoperabilitätsstatus transparent offenzulegen. Fehlende Zertifizierung wäre dabei kein Verkaufsverbot – würde jedoch Markttransparenz über Migrationsfähigkeit, Standardkonformität und praktische Austauschbarkeit schaffen.

Kopplung an den CADA: Die Souveränitätsstufen des CADA könnten mittelfristig an Interoperabilitätsnachweise gebunden werden — etwa so, dass Dienste der CADA-Stufen 2 bis 4 mindestens eine Zertifizierung der Stufe II voraussetzen und Dienste der Stufe 4 zusätzlich einen Nachweis der Wechselfähigkeit nach Stufe III. Gerade die höchste Souveränitätsstufe sollte nicht ohne erprobte Ersetzbarkeit erreichbar sein. Damit würde neben der Frage, wie stark ein Dienst Drittstaaten ausgesetzt ist, auch die Frage geprüft, ob er sich ersetzen lässt.

Finanzierung

Das Zertifizierungssystem sollte sich primär über Zertifizierungsgebühren finanzieren – analog zu bestehenden Konformitäts- und Prüfverfahren in anderen Industriebereichen.

Besonders wichtig ist dabei: Interoperabilitätszertifizierung darf nicht selbst zur Markteintrittsbarriere werden. Für Open-Source-Projekte, kleine und mittlere Anbieter sowie gemeinwohlorientierte digitale Infrastrukturprojekte sollten daher reduzierte Gebührenmodelle vorgesehen werden.

Die Entwicklung offener Test-Suites, Referenzimplementierungen und interoperabler Prüfwerkzeuge könnte zusätzlich durch europäische Forschungs- und Innovationsprogramme kofinanziert werden.

Zeitplan

Der konkrete Einführungszeitplan ist Gegenstand politischer Abstimmung zwischen EU-Kommission, Mitgliedstaaten und Normungsorganisationen. Als Orientierungsrahmen erscheint folgende Stufung realistisch:

- *Phase 1 (Jahr 1–2)*: Aufbau des Zertifizierungsrahmens, Entwicklung offener Test-Suites und Pilotbetrieb mit freiwilliger Zertifizierung
- *Phase 2 (Jahr 3–4)*: Verbindliche Beschaffungsanforderung der Stufe I für die öffentliche Hand
- *Phase 3 (ab Jahr 5)*: Verbindliche Anforderung der Stufe II für sicherheitskritische und archivierungspflichtige Systeme sowie Verknüpfung mit dem CADA und mit DMA-Mechanismen für marktmächtige Anbieter

9.6 Interoperabilität als Markttransparenz

Eine europäische Interoperabilitäts-Zertifizierung würde nicht nur technische Qualität sichtbar machen, sondern vor allem strukturelle Markttransparenz schaffen.

Unternehmen und öffentliche Einrichtungen könnten dadurch besser beurteilen:

- welche Plattformen reale Wechselbarkeit ermöglichen,
- welche Systeme langfristige Abhängigkeiten erzeugen
- und welche Lösungen interoperabel und migrationsfähig bleiben.

Dadurch würde Interoperabilität von einer schwer überprüfbaren technischen Detailfrage zu einem sichtbaren Wettbewerbsmerkmal werden.

Genau darin liegt die eigentliche wirtschaftspolitische Bedeutung eines solchen Systems:
Nicht Regulierung um der Regulierung willen, sondern die Schaffung transparenter Voraussetzungen für funktionierende digitale Märkte.

9.7 Proportionalität, Offenheit und geringe Eintrittshürden

Eine europäische Interoperabilitäts-Zertifizierung kann ihre wirtschaftspolitische Wirkung nur entfalten, wenn sie selbst keine neue Markteintrittsbarriere erzeugt.

Zertifizierungsverfahren müssen daher:

- transparent,
- reproduzierbar,
- modular
- und möglichst automatisierbar gestaltet werden.

Besonders für kleine und mittlere europäische Anbieter wäre ein hochkomplexes oder kostenintensives Zertifizierungssystem problematisch. Interoperabilitätsregulierung darf bestehende Marktkonzentrationen nicht unbeabsichtigt weiter verstärken.

Gerade dominante Plattformanbieter verfügen über erhebliche organisatorische und finanzielle Ressourcen, um komplexe Compliance- und Zertifizierungsprozesse zu bewältigen. Kleine Anbieter, Open-Source-Projekte und europäische Spezialanbieter besitzen diese Möglichkeiten häufig nicht im gleichen Ausmaß.

Ein funktionierendes Zertifizierungsmodell muss deshalb bewusst niedrige Eintrittshürden schaffen.

Dazu gehören insbesondere:

- offene und öffentlich dokumentierte Test-Suites,
- standardisierte Referenztests,
- reproduzierbare Prüfverfahren,
- modulare Zertifizierungsbausteine
- sowie weitgehend automatisierbare Konformitätsprüfungen.

Zertifizierungen sollten nicht ausschließlich durch aufwendige Einzelprüfungen erfolgen, sondern möglichst stark auf:

- offene technische Tests,
- standardisierte Validierungsverfahren
- und transparente Konformitätskriterien

aufbauen.

Dabei erscheint ein gestuftes Modell sinnvoll:
Einfache Standardimplementierungen sollten mit geringem Aufwand zertifizierbar sein, während komplexe Plattformökosysteme entsprechend umfangreichere Interoperabilitätsnachweise erbringen müssen.

Besonders wichtig ist dabei:
Die eigentliche Referenz darf nicht durch einzelne dominante Marktimplementierungen definiert werden, sondern durch offene, nachvollziehbare und reproduzierbare technische Kriterien.

Interoperabilitäts-Zertifizierung darf nicht selbst zum Lock-in werden. Ihr Ziel muss die Senkung von Wechselbarrieren sein – nicht die Schaffung neuer regulatorischer Abhängigkeiten.

10 Öffentliche Beschaffung als strategischer Hebel

10.1 Die öffentliche Hand als Marktgestalter

Die öffentliche Hand zählt in Europa zu den größten Nachfragern digitaler Technologien. Öffentliche Verwaltungen, Bildungseinrichtungen, Gesundheitssysteme und staatsnahe Organisationen investieren jährlich Milliardenbeträge in:

- Software,
- Cloud-Dienste,
- Kollaborationsplattformen
- und digitale Infrastruktur.

Beschaffung ist damit nicht nur eine operative Verwaltungsfunktion, sondern ein zentraler wirtschaftspolitischer Hebel. Öffentliche Ausschreibungen beeinflussen:

- technologische Standards,
- Marktstrukturen,
- Innovationsdynamik
- und langfristige Plattformabhängigkeiten.

Gerade im digitalen Bereich entstehen dadurch erhebliche strukturelle Effekte. Wenn öffentliche Institutionen Plattformökosysteme beschaffen, die nur eingeschränkt interoperabel oder migrierbar sind, verstärken sie bestehende Lock-in-Strukturen langfristig.

Digitale Souveränität ist daher nicht allein eine Frage technologischer Entwicklung, sondern auch eine Frage strategischer Beschaffungspolitik.

10.2 Zertifizierung als Beschaffungsvoraussetzung

Interoperabilität entfaltet ihre Wirkung nur dann, wenn sie wirtschaftlich relevant wird. Genau hier kann öffentliche Beschaffung eine zentrale Rolle spielen.

Eine europäische Interoperabilitäts-Zertifizierung könnte schrittweise als objektives Bewertungskriterium in öffentlichen Ausschreibungen etabliert werden. Ziel wäre nicht der Ausschluss einzelner Anbieter, sondern die Schaffung transparenter Anforderungen an:

- Wechselbarkeit,
- Datenmigration,
- Standardkonformität
- und praktische Interoperabilität.

Dadurch würde Interoperabilität systematisch, öffentlich nachvollziehbar und beschaffungswirksam vergleichbar.

Besonders relevant wäre dies in Bereichen mit langfristigen Abhängigkeiten:

- Dokumentenmanagement,
- Kollaborationsplattformen,
- Cloud-Services,
- Kommunikationssysteme
- und KI-gestützte Arbeitsumgebungen.

Beschaffungsentscheidungen würden dadurch nicht mehr ausschließlich kurzfristige Funktionalität bewerten, sondern auch langfristige digitale Resilienz und Migrationsfähigkeit berücksichtigen.

Der Zeitpunkt ist günstig: Am 9. September 2026 hat die Kommission vorgeschlagen, die Vergaberichtlinien von 2014 durch eine unmittelbar geltende Verordnung zu ersetzen, die unter anderem einen Rahmen für europäische Präferenzen und eine gemeinsame digitale Vergabeinfrastruktur vorsieht.[42] Die Verhandlungen in Europäischem Parlament und Rat bieten die Gelegenheit, überprüfbare Interoperabilität und erprobte Wechselfähigkeit als Eignungs- oder Zuschlagskriterium für digitale Arbeitsplatz- und Kollaborationssysteme zu verankern.

10.3 Förderung von Wettbewerb und Innovation

Interoperabilität stärkt Wettbewerb. Wenn Wechselkosten sinken und Plattformen praktisch austauschbar bleiben, entstehen:

[42] Vorschlag für eine Verordnung über öffentliche Aufträge und Konzessionen, COM(2026) 590 final vom 9. September 2026.

- niedrigere Markteintrittsbarrieren,
- größere Innovationsräume
- und mehr Wettbewerb zwischen unterschiedlichen Anbietern.

Gerade europäische Anbieter könnten davon profitieren. Heute entstehen in vielen digitalen Märkten erhebliche strukturelle Nachteile durch:

- dominante Plattformökosysteme,
- proprietäre Integrationen
- und asymmetrische Interoperabilität.

Kleine und mittlere Anbieter müssen häufig nicht nur offene Standards implementieren, sondern zusätzlich das Verhalten dominanter Plattformen nachvollziehen, um wettbewerbsfähig zu bleiben.

Verbindliche interoperable Standards und überprüfbare Konformitätsmechanismen könnten diese strukturellen Nachteile reduzieren.

Interoperabilität wird dadurch nicht zum Innovationshemmnis, sondern zur Voraussetzung funktionierender Innovationsmärkte.

10.4 Chancen für europäische Anbieter

Europa verfügt über zahlreiche leistungsfähige Anbieter in Bereichen wie:

- Cloud-Infrastruktur,
- Open-Source-Software,
- Kollaborationsplattformen,
- Sicherheitslösungen
- und digitale Verwaltungssysteme.

Viele dieser Anbieter scheitern jedoch nicht an fehlender technischer Qualität, sondern an:

- hohen Wechselkosten bestehender Plattformökosysteme,
- asymmetrischer Interoperabilität
- und mangelnder praktischer Austauschbarkeit.

Ein interoperabilitätsorientierter Beschaffungsrahmen könnte hier neue Marktchancen schaffen. Öffentliche Institutionen würden nicht primär einzelne Technologien bevorzugen, sondern Systeme, die:

- offene Standards praktisch interoperabel umsetzen,
- reale Wechselbarkeit ermöglichen
- und langfristige Plattformabhängigkeiten reduzieren.

Dadurch könnten europäische Anbieter stärker über:

- Qualität,
- Sicherheit,
- Innovation
- und Service

konkurrieren – statt primär gegen bestehende Lock-in-Strukturen.

10.5 Langfristige Archivierung und Nachhaltigkeit

Öffentliche Beschaffung betrifft nicht nur aktuelle Produktentscheidungen, sondern häufig digitale Infrastrukturen mit jahrzehntelanger Lebensdauer.

Dokumente, Verwaltungsdaten, wissenschaftliche Informationen und organisatorisches Wissen müssen langfristig:

- lesbar,
- migrierbar
- und unabhängig von einzelnen Plattformökosystemen nutzbar bleiben.

Fehlende Interoperabilität erzeugt dabei erhebliche Risiken:

- steigende Migrationskosten,
- langfristige Herstellerabhängigkeiten,
- Verlust semantischer Informationen
- oder eingeschränkte Archivierungsfähigkeit.

Gerade im öffentlichen Bereich entsteht dadurch ein Zielkonflikt zwischen kurzfristiger Funktionalität und langfristiger digitaler Resilienz.

Interoperabilität wird unter diesen Bedingungen zu einer Frage nachhaltiger staatlicher Infrastrukturpolitik.

Die öffentliche Hand besitzt daher nicht nur die Möglichkeit, sondern auch die Verantwortung, interoperable und migrationsfähige digitale Systeme aktiv zu fördern.

Öffentliche Beschaffung kann dadurch zu einem zentralen Instrument werden, um:

- Wettbewerb,
- digitale Souveränität
- und langfristige technologische Resilienz

strukturell zu stärken.

11 Handlungsempfehlungen

Die vorangegangenen Kapitel haben gezeigt, dass digitale Souveränität nicht allein durch europäische Infrastruktur oder formale Standardisierung erreicht werden kann. Entscheidend ist ob digitale Systeme langfristig interoperabel, migrierbar und praktisch austauschbar bleiben.

Die konkreten Vorschläge sind in Kapitel 9 und 10 ausgeführt. Dieses Kapitel richtet die zentralen Handlungsempfehlungen explizit an die relevanten Adressaten.

Vorbemerkung zur Terminologie

Microsoft Office bezeichnet das meistgenutzte Bürosoftwarepaket in europäischen Unternehmen und öffentlichen Institutionen – bestehend aus Word, Excel, PowerPoint und Outlook. Es wird sowohl als Einzellizenz (Microsoft Office 2024) als auch als Cloud-Abonnement unter der Bezeichnung Microsoft 365 – mit oder ohne KI-Erweiterung Copilot – vertrieben. Die Marktmacht von Microsoft Office besteht unabhängig von der jeweiligen Lizenzierungsform und unabhängig von produktbezogenen Umbenennungen. Im Kontext dieses Papiers bezeichnet „Microsoft Office" das Produkt in allen seinen Vertriebsformen.

Microsoft Office dominiert den Markt für Bürosoftware in europäischen Unternehmen und öffentlichen Einrichtungen. Eine Analyse von Compass Lexecon im Auftrag der Open Cloud Coalition schätzt den Anteil von Microsoft am Markt für Produktivitätssoftware im öffentlichen Sektor der EU auf rund 77 %, im Segment der Office-Anwendungen auf bis zu 90 %.[43] Google Workspace folgt mit deutlichem Abstand. Alle übrigen Anbieter — darunter LibreOffice, OnlyOffice und andere europäische Lösungen — teilen sich den verbleibenden Rest.

Hohe Marktanteile sind für sich genommen nicht problematisch.

Funktionierende Märkte setzen reale Wechselbarkeit voraus.
Wenn Plattformökosysteme durch proprietäre Integrationen, Workflow-

[43] Compass Lexecon (2025): Quantifying EU public sector dependence on productivity software, im Auftrag der Open Cloud Coalition. Die Werte sind Schätzungen auf Grundlage kommerzieller Marktdaten und öffentlicher Vergabedaten; Auftraggeberin ist eine Interessenvertretung. Zum gemeinsamen Anteil von Microsoft und Google bei Collaboration-Software siehe Illsinger, W. (2026): Digitale Souveränität in Europa. Definition, Status, Handlungsoptionen. Policy Brief Nr. 2026-001, Version 3. Wien: 4future.institute. DOI: 10.5281/zenodo.24042085. Abschnitt 2.2.

Abhängigkeiten und semantische Bindungen praktisch kaum mehr austauschbar sind, verliert Wettbewerb seine disziplinierende Wirkung.

11.1 An die Europäische Kommission

Erweiterung des Digital Markets Act um verbindliche Interoperabilitätsanforderungen für:

- **digitale Arbeits- und Kollaborationsplattformen –** insbesondere für Dokumentformate, Kalender- und Kontaktprotokolle sowie programmatische Schnittstellen und Interoperabilität zwischen den Diensten
- **Cloud-Infrastrukturstandards und APIs –** insbesondere dort wo proprietäre Schnittstellen faktische Marktstandards ohne regulatorische Basis geworden sind
- **KI-Plattformökosysteme und semantische Wissenssysteme –** insbesondere dort wo proprietäre KI-Agenten und Wissensmodelle neue Formen migrationsinduzierter Plattformbindung erzeugen

Prüfung, ob Microsoft Office — vertrieben als Einzellizenz und als Cloud-Abonnement unter der Bezeichnung Microsoft 365 — als zentraler Plattformdienst erfasst und Microsoft dafür als Gatekeeper benannt werden kann: als Cloud-Computing-Dienst in seiner Form als Microsoft 365 oder, falls erforderlich, durch eine Ergänzung der Liste zentraler Plattformdienste. Eine solche Ergänzung kann eine Marktuntersuchung nach Art. 19 DMA vorbereiten; beschließen müsste sie der Gesetzgeber. Microsoft ist für andere Dienste bereits als Gatekeeper benannt; die in Kapitel 4 dokumentierten Lock-in-Effekte durch asymmetrische Interoperabilität entsprechen dem Schutzzweck des DMA. Die laufende Marktuntersuchung zur Anwendung des DMA auf Cloud-Dienste sollte ausdrücklich auch Büro- und Kollaborationsdienste einbeziehen, die als Software-as-a-Service angeboten werden.

Prüfung der Gatekeeper-Designation für weitere Plattformen die trotz Erfüllung quantitativer DMA-Schwellenwerte bislang nicht designiert wurden – insbesondere dort wo De-facto-Standards ohne regulatorische Basis entstanden sind oder migrationsinduzierte Plattformbindung Wechselbarkeit strukturell verhindert.

Erteilung eines Normungsauftrags nach Verordnung (EU) Nr. 1025/2012 an CEN, CENELEC und ETSI zur Entwicklung eines europäischen Interoperabilitäts-Zertifizierungsrahmens auf Basis bestehender Normungs- und Akkreditierungsstrukturen — unter Einbindung des Interoperable Europe Board und der Erfahrungen der ENISA mit dem europäischen Rahmen für Cybersicherheitszertifizierung.

Verbindliche Transparenzpflicht für Anbieter digitaler Arbeitsplatz- und Kollaborationslösungen hinsichtlich ihres Interoperabilitätsstatus – als Grundlage informierter Beschaffungsentscheidungen öffentlicher und privater Institutionen.

Kopplung der Souveränitätsstufen des CADA an Interoperabilitätsnachweise in den Verhandlungen über COM(2026) 502 — mit dokumentierter Datenportabilität, offenen Formaten und einem erprobten Ausstiegsplan auf jeder Stufe.

Verankerung überprüfbarer Interoperabilität und erprobter Wechselfähigkeit als Eignungs- oder Zuschlagskriterium in der vorgeschlagenen Vergabeverordnung COM(2026) 590.

Veröffentlichung der Ergebnisse der Treuhänderüberwachung zu den Teams-Zusagen in einer Form, die Dritten eine Überprüfung der zugesagten Interoperabilität erlaubt.

11.2 An die österreichische Bundesregierung und EU-Mitgliedstaaten

Einführung von Interoperabilitätszertifizierung als Beschaffungsvoraussetzung für öffentliche Vergaben digitaler Arbeitsplatz- und Kollaborationssysteme – schrittweise beginnend mit einer Zertifizierung der Stufe I.

Beauftragung von Austrian Standards International mit der Entwicklung eines nationalen Pilotprogramms für Interoperabilitätszertifizierung – als Grundlage für einen europäischen Zertifizierungsrahmen.

Förderung offener Referenzimplementierungen und Test-Suites im Rahmen nationaler Digitalprogramme – insbesondere für IMAP, CalDAV, CardDAV, ODF und OOXML Strict.

Aktive Einbringung des Themas überprüfbarer Interoperabilität in die europäische Digitalpolitik — insbesondere in die Umsetzung des Interoperable

Europe Act und in die Verhandlungen über den CADA und die Vergabeverordnung.

11.3 An Normungs- und Standardisierungsorganisationen

Entwicklung standardisierter Compliance-Tests für offene Protokolle – IMAP, CalDAV, CardDAV, ODF, OOXML Strict – als öffentlich zugängliche Test-Suites.

Aufbau eines europäischen Netzwerks akkreditierter Interoperabilitätsprüfstellen unter einem gemeinsamen Rahmenwerk – analog zu bestehenden Konformitätsbewertungssystemen.

Aktive Beteiligung an der Weiterentwicklung des Interoperable Europe Act sowie an europäischen Normungsprozessen im Bereich digitaler Arbeitsplatz- und Kollaborationssysteme.

Entwicklung eines gestuften Zertifizierungsmodells mit niedrigen Eintrittshürden – insbesondere für Open-Source-Projekte und kleine Anbieter.

11.4 An die Zivilgesellschaft und Wissenschaft

Systematische Dokumentation und Publikation von Interoperabilitätsmängeln in realen Arbeitsumgebungen – als Grundlage evidenzbasierter Regulierung.

Aufbau offener Test-Suites und Referenzimplementierungen als digitales Gemeingut – gefördert durch europäische Forschungs- und Innovationsprogramme wie Horizon Europe.

Unabhängige wissenschaftliche Begleitung des Zertifizierungsprozesses – zur Sicherstellung technischer Neutralität und Herstellerunabhängigkeit.

12 Schlussfolgerung

Die europäische Diskussion über digitale Souveränität konzentrierte sich in den vergangenen Jahren vor allem auf:

- Infrastruktur,
- Cloud-Plattformen,
- Datenschutz
- und geopolitische Abhängigkeiten.

Diese Perspektive bleibt wichtig. Sie greift jedoch zu kurz.

Digitale Abhängigkeit entsteht heute zunehmend nicht nur auf Ebene von Rechenzentren oder Datenstandorten, sondern innerhalb digitaler Arbeits- und Wissensökosysteme:

- in Dokumentformaten,
- APIs,
- Kollaborationsplattformen,
- Workflow-Systemen
- und semantischen KI-Strukturen.

Gerade dort entscheidet sich, ob digitale Systeme langfristig:

- interoperabel,
- migrationsfähig
- und praktisch austauschbar bleiben.

Die zentrale Erkenntnis dieses Papiers lautet daher:

Offene Standards allein reichen nicht aus.

Standards entfalten ihre wirtschaftliche und gesellschaftliche Wirkung nur dann, wenn:

- ihre Implementierung interoperabel bleibt,
- ihre Konformität überprüfbar ist
- und reale Wechselbarkeit zwischen Plattformen möglich bleibt.

Fehlt diese praktische Interoperabilität, entstehen trotz formaler Offenheit:

- hohe Wechselkosten,
- strukturelle Lock-in-Effekte
- und langfristige Marktkonzentrationen.

Die Folge ist eine schleichende Verschiebung digitaler Macht:
weg von offenen Märkten,
hin zu integrierten Plattformökosystemen.

Besonders kritisch wird diese Entwicklung im Zeitalter KI-gestützter Wissenssysteme. Die nächste Generation digitaler Abhängigkeit entsteht nicht mehr nur über Dokumente oder Datenformate, sondern zunehmend über:

- semantische Modelle,
- organisatorisches Wissen,
- APIs,
- KI-Agenten
- und plattformgebundene Kontextsysteme.

Digitale Souveränität bedeutet unter diesen Bedingungen nicht nur Kontrolle über Infrastruktur oder Datenlokation. Sie bedeutet zunehmend auch:
die Fähigkeit, digitale Systeme praktisch wechseln zu können.

Interoperabilität wird damit zu einer zentralen Voraussetzung:

- funktionierender digitaler Märkte,
- technologischer Resilienz,
- langfristiger Innovationsfähigkeit
- und europäischer Handlungsfähigkeit.

Europa besitzt in diesem Bereich die Chance, einen eigenständigen regulatorischen und technologischen Weg zu entwickeln. Der Digital Markets Act hat begonnen, strukturelle Plattformmacht zu adressieren, und wird mit den Verfahren zu AWS und Azure erstmals auf Cloud-Infrastruktur ausgedehnt; die Teams-Zusagen, der Data Act und der Interoperable Europe Act setzen weitere Teilstücke. Die Frage überprüfbarer Interoperabilität digitaler Arbeits- und Wissensökosysteme bleibt jedoch weitgehend ungelöst.

Dieses Papier schlägt daher vor:

- interoperable Standards stärker praktisch zu überprüfen,
- europäische Zertifizierungsmodelle zu etablieren,
- offene Referenzimplementierungen zu fördern
- und Interoperabilität systematisch in öffentliche Beschaffung zu integrieren.

Ziel ist dabei nicht die Einschränkung technologischer Innovation.

Im Gegenteil:
Offene und überprüfbar interoperable Systeme schaffen die Grundlage für:

- Wettbewerb,
- Innovation,
- Marktvielfalt
- und langfristige digitale Resilienz.

Interoperabilität ist damit keine technische Randfrage. Sie entwickelt sich zu einer der zentralen industrie-, wirtschafts- und gesellschaftspolitischen Herausforderungen digitaler Gesellschaften.

Die entscheidende Frage lautet künftig nicht mehr allein:

> „Sind Standards offen?“

Sondern:

> „Ermöglichen sie reale digitale Freiheit?“

Standards ohne überprüfbare Konformität sind keine Standards. Sie sind Versprechen.

I. Über den Autor

Ing. Werner Illsinger, MBA, ist Gründer und Executive Director des 4future.institute. Er arbeitete 18 Jahre für Microsoft — von der Ära des Personal Computers bis in die Zeit der Cloud-Dominanz. Er hat erlebt, wie aus einem Unternehmen, das einst den PC demokratisiert hat, eine globale Plattforminfrastruktur wurde, die heute zentrale gesellschaftliche Funktionen kontrolliert — und zieht daraus Konsequenzen für Europa.

Ausgebildet als Nachrichtentechniker und Wirtschaftspsychologe verbindet er technisches Systemverständnis mit systemischer und gesellschaftlicher Perspektive. Dieses Papier ist kein Auftrag — es ist das Ergebnis einer wachsenden Überzeugung, dass Europa die strukturellen Bedingungen seiner digitalen Zukunft jetzt gestalten muss, solange das Fenster noch offen ist.

II. Anhang: Begriffsbestimmungen

API (Application Programming Interface)

Eine API ist eine definierte Schnittstelle, über die unterschiedliche Software-Systeme miteinander kommunizieren können. APIs legen fest, wie Anwendungen Daten austauschen oder Funktionen anderer Systeme nutzen.

Im Kontext digitaler Plattformökonomie werden APIs zunehmend zu strategischen Kontrollpunkten digitaler Ökosysteme.

Asymmetrische Interoperabilität

Asymmetrische Interoperabilität beschreibt eine Situation, in der Systeme zwar grundsätzlich miteinander funktionieren, jedoch nicht gleichwertig.

Die dominante Plattform bietet dabei typischerweise:

- den größten Funktionsumfang,
- die höchste Integrationstiefe,
- die konsistenteste Benutzererfahrung
- und die geringsten Risiken.

Alternative Anbieter bleiben formal kompatibel, tragen jedoch häufig höhere Interoperabilitäts- und Reputationsrisiken.

Austauschbarkeit

Austauschbarkeit bezeichnet die praktische Möglichkeit, digitale Systeme oder Plattformen ohne unverhältnismäßige technische, wirtschaftliche oder organisatorische Hürden wechseln zu können.

Austauschbarkeit umfasst mehr als reine Datenexportfähigkeit. Entscheidend ist, ob:

- Dokumente,
- Workflows,
- Metadaten,
- organisatorische Abläufe
- und semantische Strukturen

praktisch migrierbar bleiben.

CalDAV

CalDAV ist ein offener Standard zur Synchronisation von Kalenderdaten zwischen unterschiedlichen Systemen.

CalDAV ermöglicht unter anderem:

- gemeinsame Kalender,
- Terminverwaltung,
- Einladungen
- und plattformübergreifende Synchronisation.

CardDAV

CardDAV ist ein offener Standard zur Synchronisation von Kontakt- und Adressbuchdaten.

Der Standard ermöglicht den interoperablen Austausch von Kontaktdaten zwischen unterschiedlichen Plattformen und Anwendungen.

Compliance-Test

Ein Compliance-Test überprüft, ob ein technischer Standard tatsächlich korrekt und interoperabel implementiert wurde.

Im Gegensatz zu rein formaler Standardunterstützung bewertet ein Compliance-Test das praktische Verhalten eines Systems.

Datenportabilität

Datenportabilität bezeichnet die Möglichkeit, Daten aus einem System zu exportieren und in ein anderes System zu übertragen.

Datenportabilität allein garantiert jedoch noch keine vollständige Wechselbarkeit oder Interoperabilität.

De-facto-Standard

Ein De-facto-Standard ist ein Standard, der sich in der Praxis durch Marktverbreitung etabliert hat, unabhängig davon, ob er offiziell normiert wurde.

Dominante Plattformimplementierungen entwickeln sich häufig zu De-facto-Standards.

Digital Markets Act (DMA)

Der Digital Markets Act ist eine europäische Regulierung zur Begrenzung struktureller Marktmacht großer digitaler Plattformanbieter („Gatekeeper“).

Der DMA enthält unter anderem Vorgaben zu:

- Interoperabilität,
- Datenportabilität,
- Plattformöffnung
- und Wettbewerbsverhalten.

Digitale Souveränität

Digitale Souveränität bezeichnet die Fähigkeit von Staaten, Organisationen und Individuen, digitale Technologien unabhängig, kontrollierbar und langfristig handlungsfähig nutzen zu können.

Dazu gehören unter anderem:

- Kontrolle über Infrastruktur,
- Datenhoheit,
- Wechselbarkeit digitaler Systeme,
- Interoperabilität
- und technologische Resilienz.

Funktionale Gleichwertigkeit

Begriff des Data Act (Art. 2 Nr. 37): Ein Dienst desselben Typs liefert nach dem Anbieterwechsel bei gleichen Eingaben für die gemeinsamen Funktionen im Wesentlichen vergleichbare Ergebnisse. Der Data Act verlangt die Unterstützung funktionaler Gleichwertigkeit nur von Anbietern von Infrastrukturdiensten (IaaS).

Gatekeeper

Gatekeeper sind besonders große digitale Plattformanbieter mit struktureller Marktmacht.

Der Begriff wird insbesondere im Digital Markets Act verwendet.

Gatekeeper kontrollieren häufig zentrale digitale Zugänge oder Plattformökosysteme.

IMAP

IMAP („Internet Message Access Protocol“) ist ein offener Standard für den Zugriff auf E-Mail-Postfächer.

IMAP ermöglicht die Synchronisation von E-Mails zwischen unterschiedlichen Geräten und Mailservern.

Interoperabilität

Interoperabilität bezeichnet die Fähigkeit unterschiedlicher Systeme, Anwendungen oder Plattformen, konsistent und austauschbar zusammenzuarbeiten.

Praktische Interoperabilität bedeutet, dass definierte Funktionen in festgelegten Anwendungsfällen zwischen unabhängigen Implementierungen innerhalb vereinbarter Toleranzen übereinstimmend funktionieren — einschließlich des vollständigen Bearbeitungszyklus.

Interoperable Europe Act

Verordnung (EU) 2024/903 über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union. Sie verpflichtet öffentliche Stellen unter anderem zu Interoperabilitätsbewertungen, bevor sie verbindliche Anforderungen an transeuropäische digitale öffentliche Dienste festlegen.

ISO-Standard

Ein ISO-Standard ist eine international standardisierte technische Norm der International Organization for Standardization (ISO).

ISO-Standards definieren gemeinsame technische Spezifikationen und sollen Interoperabilität und Austauschbarkeit fördern.

KI-Agent

Ein KI-Agent ist ein softwaregestütztes System, das autonom oder teilautonom Aufgaben ausführen, Entscheidungen vorbereiten oder Arbeitsprozesse steuern kann.

KI-Agenten greifen häufig auf:

- Dokumente,
- APIs,
- Kommunikationssysteme,
- Kalender
- und Wissensmodelle

zu.

Kollaborationsplattform

Eine Kollaborationsplattform ist eine integrierte digitale Arbeitsumgebung für:

- Kommunikation,
- Dokumentenbearbeitung,
- Meetings,
- Workflow-Steuerung,
- Aufgabenverwaltung
- und Zusammenarbeit.

Beispiele sind Plattformen wie Microsoft Teams, SharePoint oder vergleichbare Arbeitsökosysteme.

Lock-in-Effekt

Ein Lock-in-Effekt beschreibt eine Situation, in der der Wechsel eines Systems oder Plattformanbieters mit hohen technischen, organisatorischen oder wirtschaftlichen Kosten verbunden ist.

Lock-in entsteht häufig durch:

- proprietäre Erweiterungen,
- fehlende Interoperabilität,
- Workflow-Abhängigkeiten
- oder Netzwerkeffekte.

Metadaten

Metadaten sind strukturierte Zusatzinformationen über Daten oder Dokumente.

Beispiele sind:

- Autoreninformationen,
- Versionshistorien,
- Freigaben,
- Zeitstempel
- oder Berechtigungen.

Netzwerkeffekt

Ein Netzwerkeffekt entsteht, wenn der Nutzen eines Systems mit der Anzahl seiner Nutzer steigt.

Digitale Plattformmärkte weisen häufig starke Netzwerkeffekte auf.

ODF (OpenDocument Format)

ODF ist ein offener und ISO-standardisierter Dokumentenstandard für Texte, Tabellen und Präsentationen.

ODF wurde entwickelt, um langfristige Herstellerunabhängigkeit und interoperable Dokumentenformate zu ermöglichen.

OOXML (Office Open XML)

OOXML ist ein XML-basierter Dokumentenstandard für Office-Dokumente.

OOXML wurde von Microsoft entwickelt und 2008 als ISO/IEC-Standard standardisiert.

Der Standard existiert in den Varianten „Strict“ und „Transitional“.

Plattformökonomie

Plattformökonomie beschreibt digitale Märkte, in denen Plattformanbieter als zentrale Vermittler zwischen unterschiedlichen Marktteilnehmern agieren.

Plattformen profitieren häufig von:

- Netzwerkeffekten,
- Integrationsvorteilen,
- Datenaggregation
- und Lock-in-Effekten.

Proprietäre Erweiterung

Eine proprietäre Erweiterung ergänzt einen offenen Standard um zusätzliche Funktionen, die nur innerhalb eines bestimmten Plattformökosystems vollständig unterstützt werden.

Dadurch kann formale Offenheit bestehen bleiben, während praktische Austauschbarkeit eingeschränkt wird.

Referenzimplementierung

Eine Referenzimplementierung ist eine technische Umsetzung eines Standards, die als objektiver Vergleichsmaßstab dient.

Referenzimplementierungen helfen dabei:

- Interpretationsspielräume zu reduzieren,
- Interoperabilität zu prüfen
- und Konformität überprüfbar zu machen.

S3 (Simple Storage Service)

S3 ist ein von Amazon entwickelter Cloud-Speicherdienst für objektbasierten Datenspeicher.

Die S3-API entwickelte sich in den vergangenen Jahren faktisch zum De-facto-Standard für objektbasierte Cloud-Speicherlösungen.

Viele Anbieter werben daher mit „S3-Kompatibilität“.

Semantische Plattform

Eine semantische Plattform verarbeitet nicht nur Daten, sondern interpretiert deren Bedeutung, Kontext und Beziehungen.

Solche Plattformen spielen insbesondere im Bereich KI-gestützter Wissenssysteme eine zentrale Rolle.

Standard

Ein Standard definiert gemeinsame technische Regeln oder Spezifikationen, um Interoperabilität, Austauschbarkeit und Kompatibilität zwischen unterschiedlichen Systemen zu ermöglichen.

Standardisierung

Standardisierung bezeichnet den Prozess der Definition und Vereinheitlichung technischer Regeln oder Formate.

Standardisierung allein garantiert jedoch noch keine praktische Interoperabilität.

Workflow-Lock-in

Workflow-Lock-in beschreibt eine Form digitaler Abhängigkeit, bei der organisatorische Abläufe, Automatisierungen und Prozesslogiken eng an ein bestimmtes Plattformökosystem gebunden sind.

Die eigentliche Wechselbarriere entsteht dabei weniger durch Datenformate als durch integrierte Arbeitsprozesse.

III. Anhang: Quellen & Literatur

Rechtsakte und Rechtsetzungsvorschläge der EU

Verordnung (EU) 2022/1925 über bestreitbare und faire Märkte im digitalen Sektor (Digital Markets Act).

Verordnung (EU) 2023/2854 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Data Act).

Verordnung (EU) 2024/903 über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union (Interoperable Europe Act).

Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie).

Richtlinie (EU) 2022/2380 (einheitliches Ladegerät).

Verordnung (EU) Nr. 1025/2012 zur europäischen Normung.

Europäische Kommission (2026): Vorschlag für einen Cloud and AI Development Act, COM(2026) 502 final, 3. Juni 2026.

Europäische Kommission (2026): Vorschlag für eine Verordnung über öffentliche Aufträge und Konzessionen, COM(2026) 590 final, 9. September 2026.

Europäische Kommission (2017): Neuer Europäischer Interoperabilitätsrahmen (EIF), COM(2017) 134.

Entscheidungen und Verfahren der Europäischen Kommission

Benennungsbeschluss Microsoft nach dem DMA vom 5. September 2023; Beschluss C(2024) 806 vom 12. Februar 2024 (Bing, Edge, Microsoft Advertising), ABl. C/2024/2709.

Commission accepts commitments offered by Microsoft to address competition concerns related to Teams, 12. September 2025 (AT.40721, AT.40873).

Marktuntersuchungen zu Cloud-Computing-Diensten nach dem DMA, 18. November 2025; vorläufige Auffassung zu AWS und Microsoft Azure, 25. Juni 2026 (IP/26/1444).

Normen und Spezifikationen

ISO/IEC 26300 – Open Document Format for Office Applications (ODF).

ISO/IEC 29500 – Office Open XML File Formats; Ecma-376.

RFC 1064 (1988); RFC 3501 (2003); RFC 9051 (2021) – Internet Message Access Protocol (IMAP).

RFC 4791 (2007) – Calendaring Extensions to WebDAV (CalDAV); RFC 6352 (2011) – CardDAV.

Unternehmensdokumentation und Dokumentation zu Dokumentstandards

Microsoft 365 Message Center (2026): MC1227454 – Exchange Web Services (EWS) retirement update, 5. Februar 2026.

Microsoft Learn: Deprecation of Exchange Web Services in Exchange Online.

Microsoft Support: Feature comparison between new Outlook and classic Outlook (laufend aktualisiert).

Microsoft Q&A: Fragen 5742426 (27. Januar 2026) und 5853986, Antworten aus dem Microsoft-Support.

Mahugh, D. (2010): Office's Support for ISO/IEC 29500 Strict. Microsoft-Blog, 6. April 2010.

Brown, A. (2010): Microsoft Fails the Standards Test. Blog, 31. März 2010.

Commonwealth of Massachusetts, Information Technology Division: Enterprise Technical Reference Model, Version 3.5 (2005) und 4.0 (2007).

Shah, R./Kesan, J./Kennis, A. (2007): Lessons for Open Standard Policies: A Case Study of the Massachusetts Experience. University of Illinois.

Outlook CalDav Synchronizer, Open-Source-Projekt der Generalize-IT Solutions OG, Wien, https://github.com/aluxnimm/outlookcaldavsynchronizer.

Microsoft Learn: Outlook doesn't support connections to Exchange by using ActiveSync (ursprünglich KB 2859522).

SmarterTools (2017): Microsoft Outlook 2016 and EAS, 4. Oktober 2017.

Microsoft Open Specifications: [MS-OI29500] Office Implementation Information for ISO/IEC 29500 Standards Support; [MS-DOCX] Word Extensions to the Office Open XML (.docx) File Format.

LibreOffice Bugzilla: Fehler 160518 (2024) und 134509 (2020); Collabora-Online-Forum, Thread 4664 (2026).

Marktdaten

Compass Lexecon (2025): Quantifying EU public sector dependence on productivity software. Im Auftrag der Open Cloud Coalition.

Microsoft (2023): Ergebnisse für das erste Quartal des Geschäftsjahrs 2024, 24. Oktober 2023.

Wissenschaftliche Literatur

Arthur, W. B. (1989): Competing Technologies, Increasing Returns, and Lock-In by Historical Events. The Economic Journal 99 (394), S. 116–131.

Farrell, J./Klemperer, P. (2007): Coordination and Lock-In: Competition with Switching Costs and Network Effects. In: Armstrong, M./Porter, R. (Hg.): Handbook of Industrial Organization, Bd. 3. Amsterdam: Elsevier, S. 1967–2072.

Rochet, J.-C./Tirole, J. (2003): Platform Competition in Two-Sided Markets. Journal of the European Economic Association 1 (4), S. 990–1029.

Shapiro, C./Varian, H. R. (1999): Information Rules: A Strategic Guide to the Network Economy. Boston: Harvard Business School Press.

Parker, G./Van Alstyne, M./Choudary, S. P. (2016): Platform Revolution. New York: W. W. Norton.

Benkler, Y. (2006): The Wealth of Networks. New Haven: Yale University Press.

Lessig, L. (2006): Code: Version 2.0. New York: Basic Books.

Wu, T. (2010): The Master Switch: The Rise and Fall of Information Empires. New York: Knopf.

Zuboff, S. (2019): The Age of Surveillance Capitalism. New York: PublicAffairs.

Cortiñas-Lorenzo, K. et al. (2024): Through the Looking-Glass: Transparency Implications and Challenges in Enterprise AI Knowledge Systems. arXiv:2401.09410.

Sharma, R. et al. (2025): Collaborative Agentic AI Needs Interoperability Across Ecosystems. arXiv:2505.21550.

Publikationen des 4future.institute

Illsinger, W. (2026): Digitale Souveränität in Europa. Definition, Status, Handlungsoptionen. Policy Brief Nr. 2026-001, Version 3. Wien: 4future.institute. DOI: 10.5281/zenodo.24042085.

4future.institute (2026): Strategie für eine lebenswerte Zukunft. 4future.institute Papers Nr. 2026-001, ISSN 3061-1903.



Gesellschaft. Wirtschaft. Technologie. Nachhaltigkeit.

Zukunft entsteht aus Balance und bewusster Gestaltung.

Das 4future.institute ist Teil der 4future.group und organisatorisch als unabhängige Einheit in der 4future business GmbH angesiedelt. Mehrheitseigentümerin ist die 4future.foundation.

Unabhängigkeit ist Voraussetzung unserer Arbeit — nicht ihr Ergebnis

4future.institute | Graben 17/10 | 1010 Wien | +43 1 31440-0 | hello@4future.institute