Policy Brief:

Digital Sovereignty Requires Verifiable Interoperability

Why Open Standards Alone Are Not Enough

Version 2
November 2026

4future.institute Policy Brief Series
Policy Brief No. 2026-002 (EN)
ISSN 3061-1881 (Online)
DOI: 10.5281/zenodo.24052138

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

This policy brief expands on Section 3.2.2 of Policy Brief No. 2026-001 "Digital Sovereignty in Europe" (Version 3, November 2026). It supersedes Version 1.1 of June 2026.

Imprint

4future.institute · Graben 17/10 · 1010 Vienna · Austria · Phone: +43 1 31440-0 · hello@4future.institute

4future.institute is part of the 4future.group and is organised as an independent unit within 4future business GmbH.

Company Register Number: FN 459359 d · Company Court: Vienna Commercial Court · VAT ID: ATU71656745 · Majority shareholder: 4future.foundation

About the 4future.institute: On almost every issue that matters today, there are more opinions than orientation. The 4future.institute asks: What is actually true here, what are the structural conditions — and does this make sense, not just economically but for us as a society? Its frame of reference is the 4future House: the goal is a good life for all, today and for future generations. It rests on three pillars, the "three Vs" — the transformation of work and the economy, distributive fairness and security of supply — linked by the rule of law, citizen-oriented administration and coordination, and founded on European fundamental values, ethics and sustainability (guiding paper "Strategie für eine lebenswerte Zukunft", 4future.institute Papers No. 2026-001, in German). Digital sovereignty is part of security of supply: being able to use digital services reliably, switch providers and decide over one's own data. The 4future.foundation enables the institute's independent work; financial support confers no influence over content or conclusions.

Series: 4future.institute Policy Brief Series, No. 2026-002 (EN), ISSN 3061-1881 (Online), DOI: https://doi.org/10.5281/zenodo.24052138

Language versions: German version: Policy Brief Nr. 2026-002 (DE), DOI: 10.5281/zenodo.24044216. In case of discrepancies, the German version prevails.

Versions: Version 1.1 (June 2026, in German); Version 2 (November 2026): included in the Policy Brief Series, revised in substance, facts and sources updated.

Disclosure: Werner Illsinger is Executive Director of the 4future.institute, managing director of 4future business GmbH and chair of the board of the 4future.foundation. He also built 4future.digital, where he serves as CTO; 4future.digital provides cloud and collaboration services as a European alternative to Microsoft 365 and Google Workspace and uses the open standards discussed in this paper. As a market participant, 4future.digital would be affected by an interoperability certification of the kind this paper proposes. 4future.digital is currently an independent company; the aim is for it to become, like 4future business GmbH, a subsidiary of the 4future.foundation. 4future business GmbH does not itself provide cloud services. The institute's recommendations are formulated in a provider-neutral way; 4future.digital and its services are neither mentioned nor assessed in the analytical part of this paper.

Executive Summary

Digital sovereignty is one of Europe's central strategic challenges. European digital policy has responded with investment in infrastructure and cloud platforms and with regulatory measures such as the Digital Markets Act (DMA). These initiatives are necessary – but so far they address one central aspect of digital dependency only inadequately:

the practical interoperability of digital systems.

Open standards have been regarded for decades as the foundation of digital sovereignty. This paper argues, however, that formal openness alone is not enough. What matters is not only that a standard exists, but that it is implemented interoperably in practice – in a way that can be verified.

The reality of digital markets shows a growing gap between:

- formal standardisation
  and
- actual interchangeability.

Document formats, APIs, collaboration platforms and communication protocols are often supported formally but implemented asymmetrically in practice. Dominant platform ecosystems typically offer the most complete and lowest-risk user experience, while alternative providers bear structural interoperability disadvantages despite supporting the standards.

The result is:

- rising switching costs,
- long-term lock-in effects
- and increasing market concentration.

The shift to AI-supported knowledge and collaboration systems intensifies this development further. The next phase of digital dependency is increasingly emerging at the level of:

- semantic knowledge models,
- platform APIs,
- AI agents
- and organisational context systems.

The paper therefore proposes a European interoperability strategy. Its key elements are:

- a European interoperability certification,
- standardised compliance tests,
- open reference implementations
- and greater weight for interoperable standards in public procurement.

The aim is not to restrict technological innovation, but to create open and competitive digital markets.

Since Version 1.1, the framework has moved: the European Commission has made Microsoft's commitments on Teams binding, which cover interoperability and data portability; it has preliminarily found that the cloud services AWS and Microsoft Azure should be designated as gatekeepers under the Digital Markets Act; and with the proposals for a Cloud and AI Development Act (CADA) and for a new procurement regulation, further instruments are on the table. None of these instruments yet requires that the practical interoperability and switchability of office and collaboration platforms be demonstrated by open, reproducible tests.

The central thesis of this paper is:

Open standards alone are not enough.
Digital sovereignty requires verifiable interoperability.

Contents

1 Introduction: The Blind Spot of Digital Sovereignty 9
1.1 Digital Resilience and Geopolitical Capacity to Act 9
1.2 Digital Sovereignty as a European Challenge 10
1.3 Infrastructure Alone Is Not Enough 11
1.4 Standards as Invisible Power Structures 11
1.5 Purpose of This Paper 13
2 Standards as the Foundation of Digital Power 14
2.1 What Standards Make Possible 14
2.2 Network Effects and the Platform Economy 14
2.3 Open vs. Proprietary Standards 15
2.4 Open Source Does Not Automatically Create Switchability 15
2.5 Formal Openness vs. Practical Interoperability 16
2.6 Standardisation Without Verifiable Conformance 16
2.7 The Difference Between Standardisation and Interchangeability 17
3 The Battle over Document Standards 19
3.1 The Historical Dominance of Proprietary Office Formats 19
3.2 The Emergence of the OpenDocument Format (ODF) 19
3.3 **Office Open XML (OOXML), ISO Standardisation and the Strict/Transitional Problem** 20
3.4 Why Document Standards Decide Digital Sovereignty 24
3.5 Long-Term Archiving and Public-Sector Dependencies 25
4 Asymmetric Interoperability in Practice 26
4.1 When Standards Are Only "Partly Open" 26
4.2 Email: IMAP as a Second-Class Citizen 26
4.3 Calendars and Contacts: CalDAV and CardDAV in Proprietary Ecosystems 27
4.4 Proprietary Extensions, APIs and Migration-Induced Platform Lock-in 29
4.5 "S3-Compatible" and Other Illusions of Interchangeability 31
5 Collaboration Platforms as a New Dependency 33

5.1 From Document to Platform 33
5.2 Teams, SharePoint and Integrated Work Ecosystems 34
5.3 Workflow Lock-in Instead of File-Format Lock-in 35
5.4 Identity, Communication and Proprietary Integration 36
5.5 Why Switching Costs Grow with Every Integration 37
6 The Blind Spot of the Digital Markets Act (DMA) 38
6.1 Aims and Mechanisms of the DMA 38
6.2 Gatekeeper Regulation and Its Limits 38
6.3 Why Workplace Standards Are Barely Addressed 40
6.4 Platform Power in the Office Rather than the App Store 40
6.5 Missing Regulatory Interoperability Mechanisms 42
6.6 European Interoperability Framework and Interoperable Europe Act 43
6.7 The Data Act: Important Progress – but Not an Adequate Answer to Modern Platform Lock-in 45
6.8 The Cloud and AI Development Act (CADA) 46
7 The Next Wave of Lock-in: AI and Semantic Platforms 48
7.1 From Documents to Knowledge Models 49
7.2 Proprietary AI Ecosystems 50
7.3 AI Agents and Semantic Dependencies 51
7.4 APIs as the New Standards 52
7.5 Risks for European Digital Sovereignty 53
8 Why Open Standards Alone Are Not Enough 54
8.1 **The Problem of Purely Formal Standardisation** 54
8.2 **Missing Compliance Testing** 54
8.3 **Missing Reference Implementations** 55
8.4 **Missing Migratability** 55
8.5 **“Open Washing” and Sham Compatibility** 55
8.6 Different Problems, Different Answers 55
9 Proposal: A European Interoperability Certification 57
9.1 Basic Idea and Objectives 57

9.2 An Independent European Certification Body 57
9.3 Technical Compliance Tests 58
9.4 Reference Implementations and Test Suites 59
9.5 Certification Levels, Enforcement and Funding 60
9.6 Interoperability as Market Transparency 64
9.7 Proportionality, Openness and Low Barriers to Entry 64
10 Public Procurement as a Strategic Lever 66
10.1 The Public Sector as a Market Shaper 66
10.2 Certification as a Procurement Requirement 66
10.3 Promoting Competition and Innovation 67
10.4 Opportunities for European Providers 68
10.5 Long-Term Archiving and Sustainability 69
11 Recommendations 70
11.1 To the European Commission 71
11.2 To the Austrian Federal Government and EU Member States 72
11.3 To Standards Bodies and Standardisation Organisations 72
11.4 To Civil Society and Academia 73
12 Conclusion 74
I. About the Author 77
II. Annex: Definitions 78
III. Annex: Sources & Literature 85
EU Legislation and Legislative Proposals 85
Decisions and Proceedings of the European Commission 85
Standards and Specifications 85
Company Documentation and Documentation on Document Standards 86
Market Data 86
Academic Literature 87
Publications of the 4future.institute 87

1 Introduction: The Blind Spot of Digital Sovereignty

1.1 Digital Resilience and Geopolitical Capacity to Act



The growing concentration of critical digital infrastructure in the hands of a few global platform providers creates not only competitive but also geopolitical risks.

European companies, administrations and public institutions today depend in central areas on non-European cloud, communication and collaboration platforms. This dependency concerns not only infrastructure but, increasingly, organisational work processes, knowledge systems and AI-supported platform ecosystems.

This creates structural vulnerabilities. Geopolitical tensions, sanctions, extraterritorial legal claims or regulatory conflicts can have a direct impact on the operational capacity of European organisations to act.

The debate on digital sovereignty must therefore not be conducted solely in terms of data protection or competition. It is increasingly also a question of strategic resilience and of Europe's long-term capacity to act.

This development is increasingly reflected in European regulatory initiatives such as the NIS2 Directive, which explicitly treats digital infrastructure as part of strategic resilience. The debate on digital sovereignty is thus no longer only about data protection or market structure, but increasingly also about the long-term operational capacity of European institutions and companies to act.

Under these conditions, digital sovereignty does not mean technological autarky. It means the ability to remain capable of acting even under geopolitical tension.

1.2 Digital Sovereignty as a European Challenge

European digital policy is responding with regulatory measures, investment in European infrastructure, data spaces, cloud initiatives and the Digital Markets Act. These initiatives are necessary and right.

So far, however, they address one central structural aspect of digital dependency only inadequately:

the practical interoperability and switchability of digital systems.

The legal framework of digital dependency — extraterritorial legal claims, the CLOUD Act, FISA Section 702, the structural limits of the EU-US Data Privacy Framework — is analysed in detail in Policy Brief No. 2026-001 "Digital Sovereignty in Europe".[1] It distinguishes four levels: legal permissibility, effectiveness of safeguards, practical capacity for control, and digital sovereignty. The present paper explores the fourth level in its technical and regulatory dimension: the question of whether digital systems remain practically interoperable and thus genuinely replaceable.

[1] Illsinger, W. (2026): Digital Sovereignty in Europe. Definition, Status, Policy Options. Policy Brief No. 2026-001 (EN), Version 3. Vienna: 4future.institute. DOI: 10.5281/zenodo.24042486.

1.3 Infrastructure Alone Is Not Enough

Digital dependency does not arise only at the infrastructure level. It arises every day – in every document that cannot be opened reliably, in every calendar that does not synchronise, in every API that presupposes proprietary extensions.

Even if data are stored in European data centres, structural dependency remains if:

- documents cannot be exchanged reliably between different systems,
- proprietary extensions define dominant market standards,
- platform switches create high operational risks
- or digital work processes remain only partly migratable.

This is particularly visible in digital document and collaboration systems. Even within individual platform ecosystems, desktop, web and mobile implementations of standardised document formats differ. Open standards such as IMAP, CalDAV or CardDAV are in some cases implemented with different functional scope and different integration quality across platform ecosystems.

The resulting interoperability risks have a direct effect on market decisions. Companies and public bodies often orient themselves towards dominant platform ecosystems because even minor compatibility deviations can create operational and reputational risks.

Dominant platform ecosystems are thus stabilised not only by product quality, but also by rising switching costs and interoperability risks.

1.4 Standards as Invisible Power Structures

Standards are the invisible infrastructure of digital markets. They define how systems communicate, how documents are interpreted, how data are stored – and how easy or difficult it is to switch platforms.

In traditional industries, standardised interfaces, certification, standardisation and verifiable interchangeability have been regarded for decades as preconditions for functioning markets. Examples such as GSM, Ethernet or the common USB-C charging port show that shared interfaces — some of them mandatory — can promote competition, innovation and market transparency.

The European Union has already recognised this importance in other areas: it has mandated a common charging port and requires gatekeepers under the

Digital Markets Act to make their messaging services interoperable.[2] For digital document and collaboration ecosystems, comparable requirements exist so far only to a limited extent.

This creates a structural problem: formal openness does not automatically lead to practical interoperability. Dominant platform implementations de facto define actual market behaviour – regardless of formal specifications or standardisation bodies.

The resulting lock-in effects affect competition, capacity for innovation, opportunities for market entry and long-term digital independence.

[2] Directive (EU) 2022/2380 (common charger); Art. 7 of Regulation (EU) 2022/1925 (Digital Markets Act).

1.5 Purpose of This Paper

This paper builds on Policy Brief No. 2026-001 and expands on its Section 3.2.2, which defines interoperability as a binding foundation of digital sovereignty and names CalDAV, CardDAV, IMAP and open document standards as minimum requirements. It substantiates this demand with documented examples, showing why the formal existence of a standard is not enough on its own. The examples are based on publicly documented cases, vendor documentation and information from vendor support. They do not replace a systematic, reproducible series of tests; the paper therefore proposes in Chapter 9 a public test corpus against which such findings can be verified.

The central thesis is: open standards alone are not a sufficient foundation for digital sovereignty — neither in its legal, nor its technological, nor its economic dimension as defined in Policy Brief No. 2026-001. What matters is their verifiable and interoperable implementation.

Building on this, the paper develops a concrete proposal for:

- European interoperability certifications,
- standardised compliance tests,
- reference implementations and
- binding interoperability requirements in public procurement.

The aim is not to restrict innovation or competition – but to enable them. Verifiable interoperability creates open, competitive and resilient digital markets.

Every standard is a good one – if only it were a standard.

2 Standards as the Foundation of Digital Power

2.1 What Standards Make Possible

Standards form the invisible infrastructure of modern digital societies. The internet itself would be inconceivable without open, standardised protocols such as TCP/IP, HTTP, SMTP or DNS. In traditional industries, too, standardised interfaces have been regarded for decades as the foundation of functioning markets: they create interchangeability, reduce switching costs and enable competition between different manufacturers.

In the digital sphere, however, standards fulfil not only a technical but also a strategic function. They determine how easily digital platforms can be switched and how open or closed digital ecosystems actually remain. Standards thus define not only technical compatibility, but increasingly also economic power relations.

Whoever controls standards often also controls access to the market.

2.2 Network Effects and the Platform Economy

Digital markets differ structurally from traditional industries. Network effects mean that dominant systems become ever more attractive the more widely they are used – often regardless of their actual technical superiority.

The more widely a particular document format, collaboration platform or API ecosystem spreads, the greater the pressure on other market participants to use the same systems. Standards play a central role here because they define how compatible alternative systems remain with the dominant platforms.

The result is markets in which existing platform ecosystems increasingly stabilise themselves. In such situations, market concentration arises not only from capacity for innovation or product quality, but also from rising switching costs and asymmetric interoperability.

In the long run, this reduces the competitive dynamics of digital markets. New providers can often translate technological innovations into market share only to a limited extent when existing platform ecosystems remain structurally protected by high switching costs.

This is particularly visible in digital knowledge work. Documents, communication systems and digital work processes must remain compatible with the dominant

platform ecosystems in order to avoid economic risks. Even minor deviations can create operational uncertainty and thus feed back directly into market decisions.

2.3 Open vs. Proprietary Standards

Formally, digital standards can be divided into open and proprietary standards. Open standards are publicly documented and can in principle be implemented by different market participants. Proprietary standards, by contrast, are controlled by individual companies and are often disclosed only in part.

In practice, however, this distinction is much less clear-cut than it first appears. Even formally open standards can contain proprietary extensions, be interpreted differently or be implemented asymmetrically. A standard can thus appear formally open and yet remain heavily dependent in practice on one dominant implementation.

This is precisely one of the central problems of digital markets: formal openness does not yet mean real interchangeability. The practical meaning of a standard is often determined less by its specification than by the dominant market implementation.

This problem is evident today in, among other things, document formats, communication protocols and calendar and contact synchronisation.

2.4 Open Source Does Not Automatically Create Switchability

Open-source-based platform models do not automatically guarantee long-term interoperability or real switchability either.

In many digital markets, hybrid models are increasingly emerging in which open base components are combined with proprietary extensions, platform-bound cloud services or commercially controlled integrations.

As a result, even formally open ecosystems can create structural dependencies – particularly when central functions, APIs or organisational workflows remain only partly interoperable or migratable.

Digital sovereignty can therefore be defined neither by licensing models nor by geographical location alone. What matters remains the practical ability to operate systems interoperably and to switch providers in reality.

2.5 Formal Openness vs. Practical Interoperability

The existence of an open standard does not guarantee practical interoperability. What matters is not only whether a specification is publicly available, but whether different implementations actually work consistently and interchangeably in practice.

In complex document and collaboration systems in particular, differences frequently arise in rendering, layout, commenting, synchronisation or workflow behaviour. Even within individual platform ecosystems, desktop, web and mobile implementations can differ.

The economic significance of such differences is often underestimated. Even minor compatibility deviations can cause operational and reputational risks. Companies and public bodies therefore often orient themselves towards dominant platform ecosystems precisely in order to minimise these risks.

This creates a structural problem for alternative providers: they bear the economic risk of possible compatibility deviations even when the cause of the deviation lies outside their own implementation. Interoperability thus becomes not only a technical challenge, but a central factor in competition.

In this way, structural lock-in effects arise that further reinforce existing platform dominance.

2.6 Standardisation Without Verifiable Conformance

Standards fully deliver their economic and social effect only if they are implemented consistently and interoperable behaviour remains verifiable in practice. Without corresponding conformance mechanisms, a paradoxical situation arises: standards exist formally – but their effect on competition remains limited.

The example of standardised document formats illustrates this problem particularly clearly. Office Open XML (OOXML) has been an ISO-standardised document format since 2008. Nevertheless, considerable differences in rendering, layout, commenting and collaboration behaviour persist between different implementations.

The standardisation of OOXML took place in a politically and economically intensely debated environment. Critics pointed, among other things, to the

complexity of the specification, the parallel existence of the already established OpenDocument Format (ODF) and the practical difficulty of interoperable implementations across different office systems.

The result is a situation in which several standardised document formats exist in parallel, while full interchangeability in practice is still achieved only to a limited extent.

The mere existence of a standard is therefore not enough to ensure open markets. Standards require verifiable conformance, interoperable reference implementations and practical compliance mechanisms. Without these, standardisation often remains formal – without fully delivering its actual market effect.

Two cases must be distinguished here. If an implementation violates mandatory requirements of the standard, its claim to conformance is unjustified; the implementation must then be corrected. If, on the other hand, the standard permits different implementations that do not fit together in relevant applications, it does not ensure the interchangeability that is needed; the standard must then be made more precise or supplemented by a binding interoperability profile.

For the customer, this distinction does not change the problem: a document cannot be reliably processed further simply because its vendor declares conformance with the standard. A standard intended to enable vendor-independent processing must be measured against this interchangeability. As with a standardised screw: it must fit the standardised nut within the specified tolerances — an "optimised" thread pitch is incompatible with a claim to conformance.

2.7 The Difference Between Standardisation and Interchangeability

Standardisation alone does not yet mean real switchability between digital platforms. A market remains open and competitive in the long term only if documents, data, processes and digital workflows remain practically migratable between different systems.

The decisive question is therefore not whether a standard exists. What matters is whether this standard enables real interchangeability between different platforms.

In many digital markets today there is a considerable gap between formal standardisation and practical switchability. This gap is further widened by network effects, the platform economy and asymmetric interoperability.

Ensuring practical interchangeability is thus not a technical detail. It is a central precondition for digital sovereignty, functioning digital markets and long-term capacity for innovation.

Standards without verifiable conformance are not standards. They are promises.

3 The Battle over Document Standards

3.1 The Historical Dominance of Proprietary Office Formats

Hardly any area of digital infrastructure shapes everyday knowledge work as strongly as document formats. Texts, spreadsheets and presentations have for decades formed the operational basis of modern companies, administrations and educational institutions. Documents contain not only information, but also business processes, contracts, decisions and institutional knowledge.

With the worldwide spread of Microsoft Office, a de facto global document standard emerged from the 1990s onwards. Formats such as DOC, XLS or PPT became for many years the dominant basis of digital office communication – long before open document standards became relevant in regulatory or political terms.

This dominance did not arise solely from technical superiority. Network effects played a central role: the more companies and institutions used the same formats, the harder it became for alternative systems to remain compatible. Documents had to work reliably with the dominant office environments in order to avoid operational risks.

This created a structural lock-in effect. Control over document formats increasingly also meant control over digital work processes themselves.

3.2 The Emergence of the OpenDocument Format (ODF)

As digital documents grew in importance, a political and economic demand for open document standards that would remain available in the long term emerged in the early 2000s. Public institutions in particular saw the danger that central government information could become dependent on individual proprietary platforms in the long run.

Against this background, the OpenDocument Format (ODF) was developed and standardised in 2006 as ISO/IEC 26300. The aim of ODF was to create a fully open, documented and vendor-independent document format that could be implemented by different office systems.

ODF was thus not only a technical project, but also an economic and socio-political signal:
documents should remain readable, exchangeable and archivable in the long term, independently of individual vendors.

The discussion about open document standards thus increasingly developed into a debate about digital sovereignty, competition, long-term archiving and the role of open standards in public institutions.

3.3 Office Open XML (OOXML), ISO Standardisation and the Strict/Transitional Problem

The political and economic context of OOXML standardisation is well documented. After the US state of Massachusetts decided in 2005 to mandate open document formats, and thus ODF, for its administration,[3] and similar considerations were being discussed in European institutions, Microsoft brought its own XML-based document format, Office Open XML, into the standardisation process. For this purpose, Ecma International set up Technical Committee TC45 in December 2005, which was to develop the specification submitted by Microsoft into a standard.[4] In 2007, Massachusetts also added Ecma-376 (Open XML) alongside ODF to its list of permitted formats.[5]

The subsequent fast-track ISO standardisation was internationally controversial. Several national standards bodies reported irregularities, such as short-notice changes in the composition of their committees ahead of the votes. South Africa, Brazil, India and Venezuela lodged formal appeals in 2008, which ISO and IEC rejected in August 2008.[6] In Norway, the standards organisation Standard Norge approved the format even though the large majority of its technical committee opposed it; in September 2008, 13 of the 23 committee members resigned in protest.[7] In Sweden, the standards organisation SIS declared its 2007 vote invalid after it had emerged that a Microsoft employee had offered partner companies incentives for their participation.[8]

OOXML was nevertheless standardised in 2008 as ISO/IEC 29500.

---

[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 December 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, press release, 15 August 2008.

[7] Norway ISO members walk out over OOXML. iTnews, October 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

The standard defines two variants: "Strict" as the cleaned-up version without the transitional features, and "Transitional" as a variant for transferring existing documents from older Microsoft Office formats. Transitional corresponds largely to the version that had failed to obtain a majority in the vote of September 2007, and was not intended for new documents. In practice, Transitional nevertheless remained the dominant implementation for many years — not only among third-party vendors, but at Microsoft itself.

Alex Brown, who had chaired the ISO Ballot Resolution Meeting in 2008 and had defended the standardisation, publicly accused Microsoft in 2010 of breaking the commitments it had made to the international standards community: the pre-release version of Office 2010, he wrote, did not support the approved Strict variant, but the format rejected in 2007.[9] Microsoft then announced that the following Office version would be able to read and write Strict. This has been possible since Office 2013; as its default format, however, Office still saves Transitional today.[10]

Transitional is part of the adopted standard ISO/IEC 29500; anyone who uses it does not leave the standard. The criticism is directed at the effect: a variant intended as a transition has become the norm and carries vendor-specific legacy forward. The name itself says what was intended. According to the rationale given in the standardisation process, the transitional features were to allow a transition period during which existing documents would retain their rendering when migrated; new documents were not to use them.[11] Almost two decades have passed since adoption in 2008. A transition that lasts this long, and in which new documents are still created in the transitional format by default, is no longer a transition but a permanent state. Part 4 of the standard (Transitional Migration Features), for example, contains compatibility settings such as autoSpaceLikeWord95 or lineWrapLikeWord6, which are intended to replicate the behaviour of historical Word versions. The 2006 Ecma edition still stated that this behaviour could not be fully described; applications had to replicate the output of the historical application. In the ISO process, these

[9] Brown, A.: Microsoft Fails the Standards Test. Blog, 31 March 2010, https://adjb.net/posts/ms-fail/.

[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.

[11] Response of Ecma TC45 in the ISO process, reproduced in: Jones, B.: suppressTopSpacingWP – Compat Settings #1. Microsoft blog, 2008, https://learn.microsoft.com/en-us/archive/blogs/brian_jones/suppresstopspacingwp-compat-settings-1

settings were described in more detail and marked as not intended for new documents.[12]

In addition, there is the vendor documentation. In a separate, continuously updated specification, Microsoft describes where Office implements ISO/IEC 29500 differently or extends it, and documents Word, Excel and PowerPoint extensions to the format in further specifications.[13] This disclosure is helpful for other implementations. But it also shows that the standard alone is not sufficient as a common basis for implementation: anyone who wants to exchange documents reliably with Microsoft Office must take into account not only ISO/IEC 29500, but also the vendor specifications and actual product behaviour.

Documented individual cases show what this means in practice:

[12] Ecma-376, 1st edition (2006), Part 4, Section 2.15.3.6 (autoSpaceLikeWord95); ISO/IEC 29500-4:2008, Transitional Migration Features, Section 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/

- **Deviation between standard and product behaviour:** According to the standard, default values are to apply to a form field without property data (ffData); according to Microsoft's own documentation, Word treats such a field as invalid, and it can be neither used nor edited. Word ignores the sub-elements label and tabIndex provided for in the standard and does not save them. According to the standard, field names may be up to 65 characters long; in Word, no more than 20.[14]
- **Vendor-specific layout rules:** Whether, with hyphenation at the end of a page or column, only the last word or the entire last line moves to the next page is controlled in Word by the settings allowHyphenationAtTrackBottom and useWord2013TrackBottomHyphenation in a Microsoft-specific namespace, documented in [MS-DOCX]. LibreOffice specifically re-implemented these settings in 2024: Word lays out the test document in the associated bug report on three pages; before the fix, LibreOffice laid it out on two.[15]
- **Version-dependent behaviour:** For an image with square text wrapping that is centred relative to the column and where text is to flow only on the larger side, Word has placed the text on the opposite side since version 2013 compared with older versions. The same DOCX document therefore appeared differently in Collabora Online and Word.[16] In an older bug report from 2020, a LibreOffice developer described replicating the layout from Word 2013 onwards as a workaround for a layout bug in Word that Microsoft should rather fix itself — a professional assessment by this developer, not an established cause of all text-wrapping problems.[17]

These cases do not prove any intention to obstruct, and not every one of them shows a breach of the standard by Microsoft. They do, however, demonstrate the mechanism: anyone who wants to exchange DOCX documents reliably with Word must take into account, besides the standard, vendor specifications, version-dependent product behaviour and ongoing compatibility fixes. The file

[14] Microsoft: [MS-OI29500], Sections 2.1.518 (Part 1 Section 17.16.17, ffData) and 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], Sections 2.3.7 and 2.3.8; LibreOffice Bugzilla, bug 160518 ("DOCX: fix layout of hyphenated text by supporting allowHyphenationAtTrackBottom and useWord2013TrackBottomHyphenation"), fixed in version 24.8; comparison based on the test file in attachment 193486 (useWord2013TrackBottomHyphenation = 1, allowHyphenationAtTrackBottom = 0): three pages in Word, two in LibreOffice before the fix. Later additions concerning export are dealt with in bug 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, bug 134509 ("FILEOPEN DOCX: Text behind image"), comment 12 of 2 December 2020.

extension DOCX on its own does not yet describe a uniform expectation of how a document will be rendered.

The structural consequence is clear: alternative providers bear additional adaptation effort in order to replicate the behaviour of the dominant implementation, and customers experience remaining deviations as a risk of switching providers. This does not require proof that deviations were created deliberately — what matters is the mechanism. The de facto reference standard is not ISO/IEC 29500 Strict, but the behaviour of Microsoft Office.

The parallel existence of ODF and OOXML as ISO standards has not produced the interoperability hoped for. It has increased complexity – and reinforced structural dependency on the dominant implementation.

3.4 Why Document Standards Decide Digital Sovereignty

Document standards are not a technical side issue. They determine how knowledge is stored, exchanged and kept usable in the long term.

When documents:

- cannot be exchanged reliably between different systems,
- can be migrated only to a limited extent
- or de facto favour particular platforms,

profound structural dependencies arise.

This becomes particularly relevant in public institutions and companies with long-term archiving and documentation obligations. There, documents often have to:

- remain readable for decades,
- be migratable between different systems
- and remain available independently of individual vendors.

A lack of practical interoperability, by contrast, leads to:

- rising switching costs,
- long-term platform dependencies
- and restricted openness to competition.

Document standards thus become a central infrastructural question of digital sovereignty.

3.5 Long-Term Archiving and Public-Sector Dependencies

The importance of open and interoperable document standards is particularly evident in the long-term archiving of government and institutional information.

Government documents, contracts, administrative files or academic works often have to remain readable for decades or even centuries. Proprietary or only partly interoperable formats create considerable risks here:

- future software dependencies,
- restricted migratability,
- loss of formatting or metadata
- and long-term loss of control over public information.

Digital sovereignty therefore means not only control over infrastructure and data locations. It also means:
the long-term ability to read, migrate and archive one's own information independently of individual platform ecosystems.

Public institutions in particular bear a special responsibility here. Their procurement decisions influence not only short-term productivity, but in the long term also:

- market structures,
- competition
- and the digital resilience of government information systems.

4 Asymmetric Interoperability in Practice

4.1 When Standards Are Only "Partly Open"

The existence of open standards often conveys an impression of technical neutrality and interchangeability. In practice, however, interoperability rarely works completely. Systems are usually neither fully open nor fully closed. Instead, hybrid platform ecosystems emerge in which standards are formally supported, but their practical implementation shows considerable differences.

In digital platform markets in particular, even partly asymmetric interoperability is enough to create strong lock-in effects. Systems work with one another in principle – but not on equal terms. Certain functions remain restricted, integrations incomplete or user experiences inconsistent.

This creates a structural market asymmetry: the dominant platform offers the most complete and lowest-risk user experience within its own ecosystem, while alternative providers are often perceived as "not fully compatible" despite supporting the standards.

Interoperability is thus formally assured, but gradually limited in practice.

4.2 Email: IMAP as a Second-Class Citizen

IMAP (Internet Message Access Protocol) has been an open standard for accessing email mailboxes for decades. It was first described in 1988 as RFC 1064; the current version, IMAP4rev2, is specified in RFC 9051 (2021), and its predecessor IMAP4rev1 in RFC 3501 (2003).[18] The standard is maintained by the Internet Engineering Task Force (IETF) and remains a central foundation of interoperable email communication to this day.

At the same time, modern platform ecosystems in particular show that formal support for a standard does not automatically mean equivalent functionality.

The new Outlook for Windows, rolled out gradually since 2023, supports IMAP and POP accounts but treats them differently from Exchange or Microsoft 365 accounts. Functions such as calendar integration, the handling of meeting

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

invitations or cross-platform collaboration are available only to a limited extent for IMAP accounts.[19]

On the official support platform Microsoft Q&A, support staff refer users who want to manage meeting invitations with IMAP accounts to the classic Outlook client or to migrating the mailbox to Microsoft 365. The reason given is that IMAP and POP only support the synchronisation of email, not of a full calendar.[20] That is true of IMAP — the open standard for calendars is CalDAV. Outlook does not support it (see Section 4.3).

Thus, for IMAP accounts in the new Outlook, calendar invitations are stored in a local calendar of the respective account, which is not synchronised with other calendars or devices.[21] For users, this results in an asymmetric user experience:

The example illustrates a fundamental pattern of modern platform markets: standards are formally supported, but integrated to different depths into the respective platform ecosystem. Interoperability thus remains – but not on equal terms.

4.3 Calendars and Contacts: CalDAV and CardDAV in Proprietary Ecosystems

CalDAV and CardDAV are open standards for calendar and contact synchronisation, specified by the Internet Engineering Task Force (IETF) in RFC 4791 (2007) and RFC 6352 (2011).[22] They are natively supported by, among others, Apple Calendar, Google Calendar, Thunderbird and the vast majority of other email and calendar clients.

Microsoft Outlook supports neither CalDAV nor CardDAV natively, in either the classic or the new client. On Microsoft Q&A in January 2026, Microsoft support

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

[20] Microsoft Q&A, question 5853986 ("Why does the new Outlook no longer support my email…"), answer from 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 January 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.

advised users who rely on CalDAV to return to classic Outlook and use the third-party extension "CalDav Synchronizer" there.[23]

This lack of native support has considerable structural effects on digital work ecosystems.

In many companies and public institutions, Outlook is the central email and calendar client. At the same time, the platform reaches its greatest depth of integration within the Microsoft 365 ecosystem. Systems based on open standards such as CalDAV and CardDAV, by contrast, can achieve this quality of integration within Outlook only to a limited extent.

The extension mentioned, "Outlook CalDav Synchronizer", is an open-source project of the Vienna-based Generalize-IT Solutions OG that retrofits the missing synchronisation to the classic Outlook client.[24] It is not available for the new Outlook client, because the latter does not support classic COM add-ins. With the replacement of the classic client, this bridge to open standards therefore also loses its basis.

Microsoft documents no native support for CalDAV or CardDAV in Outlook. Corresponding user requests have been found on official support and community platforms for many years, without a native implementation having been announced or documented.

The lack of support for open calendar and contact standards is not explicitly communicated as a refusal. In practice, however, a situation arises in which the platform's own integration mechanisms are continuously developed further, while open standard protocols receive no equivalent support within the dominant platform ecosystem.

In parallel, Exchange ActiveSync (EAS) – Microsoft's proprietary protocol for mobile email and calendar synchronisation – shows a complementary pattern. EAS is a protocol controlled and licensed by Microsoft that has been

[23] Microsoft Q&A, "New Outlook – non-MSA account calendar invites do not save to default calendar", answer by the moderators ("Microsoft External Staff") of 27 January 2026, https://learn.microsoft.com/en-us/answers/questions/5742426/

[24] Outlook CalDav Synchronizer, open-source project (AGPL) of Generalize-IT Solutions OG, Vienna, https://github.com/aluxnimm/outlookcaldavsynchronizer

implemented by numerous platforms and mobile clients in order to ensure compatibility with Exchange and Microsoft 365 environments.

Microsoft's own desktop clients, however, now hardly rely on EAS at all. According to Microsoft, Outlook does not support EAS for connections to Exchange Server; there, EAS is intended only for other services.[25] For precisely these other services, an update to Outlook 2016 (version 16.0.8431.2079 of 12 September 2017) restricted set-up: according to reports from providers of EAS-capable mail servers, the newly introduced simplified account set-up causes the creation of new EAS accounts by the usual route to fail. Accounts already set up continue to work; the earlier set-up can only be restored by an intervention in the Windows registry that disables simplified account set-up.[26] The function therefore exists, but for new accounts it can now only be used by a detour. The new Outlook for Windows does not support EAS accounts at all.[27]

This creates a structurally asymmetric situation:
open standards are supported across the industry, but not natively integrated within the dominant Outlook ecosystem. Proprietary Microsoft protocols, in turn, have been implemented by large parts of the industry, but are themselves losing importance within modern Microsoft platform architectures.

The actual platform lock-in thus arises not primarily from a lack of standardisation, but from differing quality and depth of integration. Organisations have a practical incentive to use the fully integrated platform ecosystem in order to avoid operational friction and compatibility problems.

Interoperability formally remains. In practice, however, it loses its equivalence with deeply integrated proprietary platform services.

4.4 Proprietary Extensions, APIs and Migration-Induced Platform Lock-in

A central pattern of asymmetric interoperability consists not in the outright rejection of open standards, but in their selective implementation combined with

[25] Microsoft Learn: Outlook doesn't support connections to Exchange by using ActiveSync (originally KB 2859522), applies to Outlook 2013, 2016 and 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 October 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, answer from Microsoft support, https://learn.microsoft.com/en-us/answers/questions/1827479/

proprietary extensions that create structural advantages within the dominant platform ecosystem.

This pattern can be seen in:

- document formats,
- communication protocols,
- calendar standards
- and increasingly also in programmatic interfaces (APIs) that define access to platform data and services.

The Documented Example: EWS and Microsoft Graph

Since 2007, Exchange Web Services (EWS) had been the central interface for programmatic access to Exchange mailboxes. Numerous third-party products – including backup solutions, CRM systems, calendar clients and collaboration platforms – were developed on the basis of this interface.

In 2018, Microsoft stopped the functional development of EWS. In 2023, the company announced that it would shut down EWS in Exchange Online. Under the updated timetable of February 2026, EWS has been gradually disabled since 1 October 2026; organisations can continue to use it only via an exception list for individual applications. From 1 April 2027, EWS in Exchange Online will be shut down permanently and without exceptions.[28] Exchange Server in the organisation's own data centre is not affected. Microsoft names the Microsoft Graph API as the successor.

Microsoft Graph is not a further development of an open standard, but a proprietary REST-based platform API under Microsoft's control – with its own authentication model, its own permission system and platform-specific access concepts.

Microsoft itself speaks of "near-complete" functional parity between Graph and EWS; certain functions are not available via Graph, or only in a different form.

[28] Microsoft 365 Message Center, MC1227454: Exchange Web Services (EWS) retirement update, 5 February 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

The structural consequence is technically and economically relevant: third-party vendors that have built their products on a documented interface over many years must migrate, within a fixed time window, to a proprietary platform API – with documented functional differences and without a standardised interoperable alternative.

The Pattern in Its General Form

EWS is not an isolated case, but the expression of a general platform pattern: documented or open interfaces are gradually replaced by proprietary platform architectures. The resulting migrations create:

- technical conversion costs,
- organisational dependencies
- and increasing integration complexity.

Proprietary extensions have long ceased to concern only document formats or communication protocols. They increasingly include:

- workflow logic,
- metadata,
- collaboration mechanisms,
- authentication models
- and platform-specific integrations.

The more complex digital work environments become, the harder it is for alternative providers to replicate these integrations. The actual competitive disadvantage therefore often arises not in implementing the standard itself, but in replicating the proprietary platform behaviour that surrounds the standard.

Interoperability formally remains. The structural asymmetry arises in the layer above.

4.5 "S3-Compatible" and Other Illusions of Interchangeability

The problem of asymmetric interoperability is particularly evident in so-called "compatible" platform services. A well-known example is the term "S3-compatible".

In recent years, Amazon S3 (Simple Storage Service) has in effect become the de facto standard for object-based cloud storage. Numerous European and

international providers today advertise “S3 compatibility” to signal that their storage solutions are interchangeable with existing cloud applications.

In practice, however, this compatibility often means only basic API functionality – not necessarily full equivalence in:

- permission models,
- metadata,
- performance,
- replication,
- security features
- or workflow integration.

In complex enterprise environments in particular, even small differences can have considerable operational effects.

This creates a situation in which alternative providers appear formally compatible, while the dominant platform continues to be perceived as the lowest-risk reference implementation.

The result is a structurally distorted market: interoperability exists formally, but real switchability remains limited.

Asymmetric interoperability thus becomes a central mechanism of the modern platform economy.

5 Collaboration Platforms as a New Dependency

5.1 From Document to Platform

The digital dependency of modern work environments no longer arises solely at the level of individual document formats. Whereas earlier lock-in effects centred primarily on files and proprietary formats, platform power is increasingly shifting to integrated digital work ecosystems.

Today, documents are only one component of complex collaboration platforms. Communication, calendars, identity, file storage, video conferencing, task management, permissions and workflow systems are increasingly brought together in unified platform environments.

This also changes the structure of digital dependency:
the focus is no longer on individual files, but on entire digital work processes.

Switching a platform ecosystem thus affects not only documents, but:

- communication,
- collaboration,
- identity management,
- process logic
- and organisational routines.

Switching costs therefore rise considerably (see Figure 1).

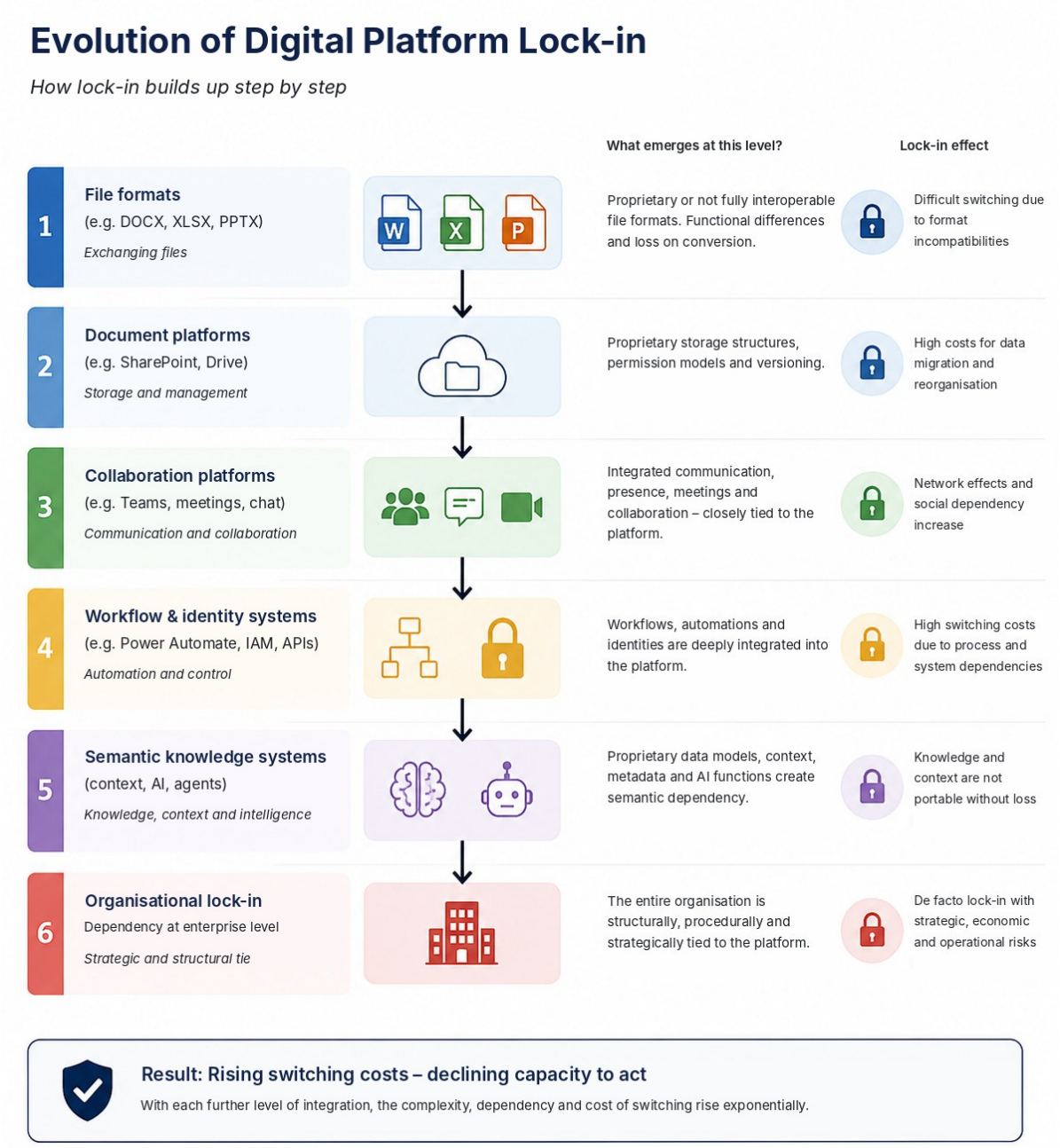


Figure 1: The evolution of digital platforms

5.2 Teams, SharePoint and Integrated Work Ecosystems

Modern collaboration platforms derive their strength above all from deep integration. Systems such as Microsoft Teams, SharePoint or comparable platform solutions combine:

- communication,
- file storage,
- rights management,
- meetings,
- collaboration
- and workflow logic

into a unified digital workspace.

Within such platforms, a consistent and highly integrated user experience emerges. At the same time, interoperability with external or alternative systems becomes increasingly complex.

Documents are only one part of a much larger platform context:

- permissions,
- comments,
- version histories,
- sharing,
- meetings,
- automations
- and AI features

are linked directly to the platform ecosystem.

This creates a new form of digital dependency:
the actual tie no longer arises primarily through document formats, but through integrated work environments.

5.3 Workflow Lock-in Instead of File-Format Lock-in

With the increasing integration of digital work processes, the nature of lock-in effects is also shifting. Whereas earlier dependencies rested mainly on proprietary file formats, modern barriers to switching increasingly arise at the level of:

- workflows,
- integrations,
- automations
- and collaboration logic.

The more closely companies adapt their work processes to a particular platform ecosystem, the harder a later switch becomes.

This becomes particularly relevant for:

- automated processes,
- AI-supported workflows,
- integrated rights management,
- communication histories
- or platform-specific extensions.

The real challenge lies less in migrating individual data sets than in restoring functioning organisational routines within a new system.

Lock-in thus increasingly arises at the semantic and organisational level – not only at the technical level.

5.4 Identity, Communication and Proprietary Integration

A key component of modern platform ecosystems is the central integration of identity and communication. User accounts, access rights, group structures, calendars, chats, meetings and collaboration features are closely interlinked.

This creates highly integrated digital work environments whose value lies not primarily in individual applications, but in the totality of their integrations.

For alternative providers, this poses a considerable challenge:
even if individual functions are available in interoperable or standards-based form, full integration often remains platform-specific.

The result is asymmetric interoperability:
alternative systems can often provide basic functions, but do not achieve the same depth of integration and consistency within the dominant platform ecosystem.

It is precisely this that gives rise to long-term dependencies that go far beyond individual software products.

5.5 Why Switching Costs Grow with Every Integration

The economic significance of modern platform ecosystems lies above all in their ability to raise switching costs continuously.

Economic research describes how switching costs and network effects can protect incumbent providers and tip markets in favour of one system.[29] In integrated platform ecosystems, there is the additional factor that ties accumulate across many services.

With every additional integration, the following grow:

- technical dependencies,
- organisational adaptations,
- training effort,
- data migrations
- and procedural ties.

At the same time, the complexity of interoperable alternatives increases. Even if individual components could be replaced technically, restoring comparable organisational routines often remains associated with considerable risks.

What is particularly problematic is the cumulative effect of these dependencies. Individual integrations often appear uncritical. Over the years, however, a highly complex platform ecosystem emerges whose complete migration becomes increasingly unrealistic in economic and organisational terms.

Digital market power thus shifts step by step:
from individual applications to integrated digital working environments.

Under these conditions, interoperability becomes not only a technical property of individual products, but a central precondition for functioning digital markets.

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

6 The Blind Spot of the Digital Markets Act (DMA)

6.1 Aims and Mechanisms of the DMA

With the Digital Markets Act (DMA), the European Union has for the first time attempted to address the structural market power of large digital platforms through regulation. The aim of the DMA is to create fair conditions for competition in digital markets and to limit dependency on so-called "gatekeepers".

The DMA targets platform companies that, by virtue of their size, reach and market position, play a central intermediary role between businesses and end users. The regulation is intended to prevent dominant platforms from using their market position to restrict competition systematically or to disadvantage alternative providers structurally.

The central mechanisms of the DMA include, among others:

- interoperability requirements,
- data portability,
- restrictions on self-preferencing within platforms
- and obligations to open certain interfaces.

The DMA thus marks an important regulatory paradigm shift:
digital markets are no longer regarded solely as spaces for innovation, but increasingly also as infrastructural power structures.

6.2 Gatekeeper Regulation and Its Limits

Despite its importance, the DMA has considerable structural limits. The regulation focuses primarily on:

- search engines,
- app stores,
- social networks,
- online advertising
- and mobile platform ecosystems.

Digital work and collaboration platforms, by contrast, are addressed less strongly – even though it is precisely there that long-term lock-in effects and high switching costs arise.

The economic significance of modern office and collaboration ecosystems goes far beyond traditional software products. They increasingly form the operational basis of:

- public administration,
- corporate knowledge work,
- internal communication
- and organisational processes.

Nevertheless, there are so far only limited regulatory requirements regarding:

- interoperable document formats,
- equivalent communication standards,
- workflow migration
- or practical interchangeability between platform ecosystems.

The DMA thus addresses platform power in the consumer sphere, but so far takes only limited account of the structural importance of digital work ecosystems.

Cloud computing services and number-independent interpersonal communications services are expressly among the DMA's core platform services. Until 2025, however, no cloud service had been designated. In November 2025, the Commission opened market investigations into whether AWS and Microsoft Azure should be designated as gatekeepers despite falling below the quantitative thresholds, as well as a third investigation into whether the DMA's obligations are adequate for cloud markets — including with regard to obstacles to interoperability.[30] On 25 June 2026, it informed Amazon and Microsoft of its preliminary view that both services should be designated; a final decision is pending (as of November 2026).[31]

These proceedings concern the infrastructure services AWS and Azure. They do not cover the office and collaboration applications built on top of them, on which the daily work of administrations and companies depends.

[30] European Commission: opening of three market investigations into cloud computing services under the Digital Markets Act, 18 November 2025.

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

6.3 Why Workplace Standards Are Barely Addressed

A key reason lies in the historical development of European platform regulation. For a long time, digital market power was defined primarily in terms of:

- search engines,
- social networks,
- e-commerce
- and mobile platforms.

Document formats, collaboration platforms and digital work processes, by contrast, were often regarded as traditional software markets – not as infrastructural power structures.

In reality, however, modern collaboration platforms have long since become central digital infrastructures. They control:

- communication,
- the organisation of knowledge,
- identity management,
- document flows
- and organisational collaboration.

It is precisely this that creates particularly strong network effects. Companies orient themselves not only towards individual applications, but increasingly towards entire work ecosystems.

The question of interoperable workplace standards thus becomes a central challenge for economic and competition policy.

6.4 Platform Power in the Office Rather than the App Store

The greatest digital dependency of European companies today often arises not in social media or mobile app stores, but within digital work environments.

Documents, meetings, chats, calendars, identity, permissions and workflows are increasingly brought together in integrated platform ecosystems. Platform power is thus shifting from individual applications to entire organisational working environments.

The switching costs of such systems differ fundamentally from those of traditional software markets. Companies no longer switch just individual programs, but potentially:

- communication structures,
- document logic,
- process landscapes,
- identity models
- and organisational knowledge systems.

It is precisely this that gives rise to new forms of structural platform lock-in that can be captured only to a limited extent by traditional indicators of competition.

The DMA Gatekeeper Question for Microsoft 365

The Digital Markets Act defines gatekeepers on the basis of quantitative thresholds such as turnover, market capitalisation and user numbers; following a market investigation, however, the Commission can also designate services below these thresholds.

Microsoft services such as Teams or Outlook achieve considerable reach in European companies and public bodies. In October 2023, Microsoft reported more than 320 million monthly active Teams users worldwide; the company has not published more recent figures.[32]

Under the DMA, Microsoft is designated as a gatekeeper for the PC operating system Windows and for LinkedIn. For the email service Outlook.com, the Commission found in 2023 that Microsoft met the quantitative thresholds, but did not designate the service because Microsoft had sufficiently substantiated that it is not an important gateway; in 2024, it excluded Bing, Edge and Microsoft Advertising for the same reason.[33] Teams and the Office applications are not designated core platform services.

This creates a situation of regulatory relevance: central components of modern work ecosystems have so far been subject only to a limited extent to the DMA's

[32] Microsoft, results for the first quarter of fiscal year 2024 (earnings call), 24 October 2023.
[33] European Commission, designation decision of 5 September 2023 (Microsoft); Decision C(2024) 806 of 12 February 2024, summary in OJ C/2024/2709.

specific interoperability obligations – even though it is precisely there that considerable structural switching costs and platform dependencies arise.

It is noteworthy that the Commission has addressed the interoperability of collaboration tools not through the DMA, but in antitrust proceedings. On 12 September 2025, it made Microsoft's commitments binding: Microsoft offers Office and Microsoft 365 suites without Teams, ensures the interoperability of key functions between competing collaboration tools and certain Microsoft products, and enables the export of Teams messaging data. The commitments on interoperability and data portability apply for ten years; a trustee monitors their implementation.[34]

This shows two things. The Commission recognises asymmetric interoperability in digital work environments as a competition problem. At the same time, the solution remains a case-specific arrangement for one company and one product, whose effectiveness third parties cannot verify by means of open, reproducible tests.

The actual market power of modern platforms increasingly arises through:

- depth of integration,
- workflow dependency,
- identity management,
- API control
- and asymmetric interoperability.

It is precisely this area that the DMA in its current form has so far covered only in part.

6.5 Missing Regulatory Interoperability Mechanisms

The DMA does contain individual interoperability requirements, but so far barely addresses the question of verifiable practical interoperability of complex work and collaboration systems.

In particular, the following are still missing:

[34] European Commission: Commission accepts commitments offered by Microsoft to address competition concerns related to Teams, press release of 12 September 2025, Cases AT.40721 and AT.40873.

- standardised compliance tests,
- interoperable reference implementations,
- regulatory conformance assessments
- and binding criteria for practical interchangeability.

This creates a regulatory gap:
standards can exist formally without their actual interoperable implementation being verified.

In highly concentrated platform markets in particular, however, formal openness is not enough. Without verifiable conformance, the following persist:

- structural lock-in effects,
- high switching costs
- and long-term market asymmetries.

The central challenge of digital sovereignty therefore lies not only in the existence of open standards, but increasingly in their practical enforceability.

The DMA has begun to address digital platform power through regulation. The question of verifiable interoperability of digital work ecosystems, however, remains largely unresolved so far.

6.6 European Interoperability Framework and Interoperable Europe Act

With the European Interoperability Framework (EIF), the European Union already has an important strategic framework for promoting interoperable digital administrative systems. The EIF defines basic principles of organisational, semantic, technical and legal interoperability within European administrative structures.

The European Union thus already recognises, in principle, the strategic importance of interoperable digital systems. The EIF addresses in particular:

- open standards,
- reusability,
- cross-border cooperation
- and long-term digital sustainability.

The framework, however, is primarily recommendatory and conceptual in character. Binding technical conformance assessments, interoperable reference

implementations or standardised compliance mechanisms for complex platform ecosystems have so far been less of a focus.

The Interoperable Europe Act added a binding legal framework in 2024. Since 12 January 2025, public bodies have had to carry out an interoperability assessment before they establish or significantly modify binding requirements for trans-European digital public services; an Interoperable Europe Board coordinates implementation.[35] The act targets the cross-border interoperability of public services. It does not examine whether the office and collaboration platforms that administrations work with are interchangeable in practice.

Modern collaboration and knowledge platforms in particular, however, now create structural dependencies that go far beyond traditional administrative interoperability. The practical switchability of integrated work environments increasingly depends on organisational workflows, platform APIs, semantic models and AI-supported context systems.

The EIF thus forms an important strategic starting point for European interoperability policy. The question of verifiable practical interoperability of complex platform ecosystems, however, has so far been addressed only to a limited extent.

[35] Regulation (EU) 2024/903 (Interoperable Europe Act), OJ L of 22 March 2024, in particular Art. 3; Interoperable Europe Portal: Interoperability assessments are now mandatory, 13 January 2025.

6.7 The Data Act: Important Progress – but Not an Adequate Answer to Modern Platform Lock-in

With the Data Act , the European Union has taken an important regulatory step towards reducing structural dependencies in digital markets. The Data Act addresses in particular data portability, cloud switching and technical barriers to switching between digital services. Providers are not to make switching artificially difficult, are to avoid excessive exit costs and are to provide standardised interfaces for data migration.

The Data Act has applied since 12 September 2025; switching charges are prohibited from 12 January 2027. The gradation of the technical obligations is revealing: only providers of infrastructure services (IaaS) must support their customers in achieving functional equivalence with the new provider. Providers of platform and software services — and thus also of office and collaboration platforms — must provide open interfaces and, as long as no common specifications have been published, export data in a structured, commonly used and machine-readable format.[36] Once common specifications or harmonised standards for the interoperability of such services have been published in the central Union repository, the services must also be compatible with them (Art. 30(3), Art. 35). Until then, for precisely the services this paper is concerned with, the Data Act requires the export of data, not equivalence of function. It remains open whether future specifications will capture the practical switchability of complex work environments — with workflows, permissions and organisational context.

In the area of cloud infrastructure and platform services in particular, this represents important progress. The measures are sensible and necessary in terms of economic policy. However, they primarily address infrastructural and data-related dependencies. The actual switchability of modern digital work ecosystems today goes far beyond this.

The structural platform lock-in of modern collaboration and knowledge systems increasingly arises not from data holdings alone, but from integrated workflows, organisational process logic, permission models, automation mechanisms, platform-specific APIs and semantic links between different services. The shift to AI-supported work environments intensifies this development further.

[36] Regulation (EU) 2023/2854 (Data Act), Art. 2(37), Art. 29 and Art. 30.

An export of files or data therefore does not yet guarantee real organisational switchability.

This is particularly evident in modern workplace and collaboration platforms. Companies today increasingly integrate document management, communication, meetings, task management, identity management and workflow automation into shared platform ecosystems. This yields considerable productivity and integration benefits. At the same time, however, organisational switching costs also rise.

The real challenge often no longer lies in migrating individual data sets, but in restoring functioning organisational routines within alternative systems. Documents can be exported without automation processes, approval workflows, integrations, permission logic or organisational context knowledge thereby automatically being migrated without loss.

The next phase of platform dependency is thus increasingly emerging at the semantic and organisational level – not solely at the level of data or infrastructure.

The Data Act has so far addressed this problem only to a limited extent; the Digital Omnibus proposed by the Commission even provides for relief for certain services that are not infrastructure services.[37] Data portability remains a necessary precondition for digital sovereignty, but it is not a sufficient condition for real switchability of complex work and knowledge platforms.

This is precisely why the question of verifiable practical interoperability is gaining further importance. In future, digital sovereignty will mean not only the ability to export data, but increasingly also the ability to keep organisational work processes, semantic knowledge structures and digital collaboration interoperable and migratable across platforms.

6.8 The Cloud and AI Development Act (CADA)

With its proposal for a Cloud and AI Development Act of 3 June 2026, the Commission is for the first time proposing sovereignty-related assurance levels for cloud services ("Union assurance levels").[38] On switching, the proposal relies

[37] European Commission proposal for a Digital Omnibus, November 2025.

[38] Proposal for a Regulation on strengthening the European cloud and AI ecosystem (Cloud and AI Development Act), COM(2026) 502 final of 3 June 2026.

on the provisions of the Data Act; at the higher levels, it requires documented migration plans. It does not, however, make a tested exit capability of the public body a general requirement, and practical interoperability is not tested.[39]

Policy Brief No. 2026-001 therefore proposes requiring documented data portability, open formats and a tested exit plan at every CADA assurance level, and linking these levels to a European interoperability certification in the medium term. Chapter 9 of this paper develops this certification.

[39] For an analysis, see Illsinger, W. (2026): Digital Sovereignty in Europe. Definition, Status, Policy Options. Policy Brief No. 2026-001 (EN), Version 3. Vienna: 4future.institute. DOI: 10.5281/zenodo.24042486. Section 2.4.

7 The Next Wave of Lock-in: AI and Semantic Platforms

The following observations describe emerging developments on the basis of current market trends. They make no claim to completeness, but are intended to point to structural risks that are already discernible today.

The debate on digital sovereignty today still focuses heavily on infrastructure:

- data centres,
- cloud platforms,
- networks
- and data location.

This perspective, however, increasingly falls short. Digital dependency is gradually shifting from pure infrastructure to integrated knowledge, context and AI systems.

Figure 2 illustrates this development using three levels of technological sovereignty:

1. digital infrastructure,
2. interaction with the physical world,
3. data and knowledge.

While the first phase of digital sovereignty concerned primarily questions of infrastructure, the most strategically relevant dependencies will increasingly arise in future at the level of semantic knowledge and AI systems.

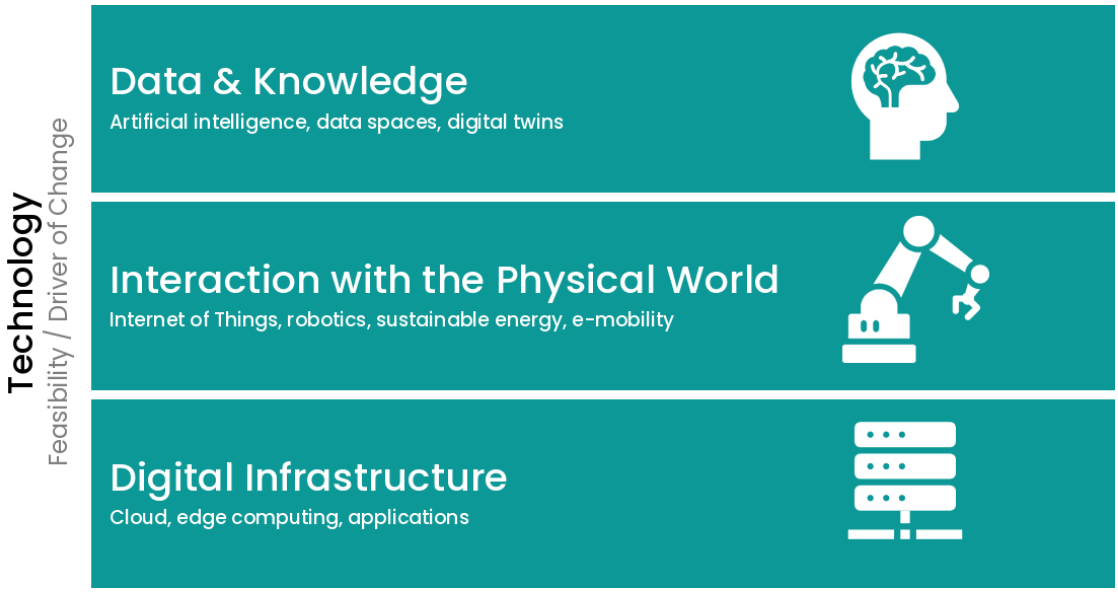


Figure 2: Levels of digital sovereignty and technological dependency

The importance of interoperable standards is thus growing considerably. Documents, communication systems, platforms and APIs are no longer just technical work tools, but increasingly the semantic foundation of AI-supported systems.

7.1 From Documents to Knowledge Models

The next phase of platform dependency no longer arises primarily at the level of individual documents or applications, but at the level of semantic knowledge models and AI-supported work processes.

Whereas earlier lock-in effects arose mainly from proprietary file formats or platform integrations, digital dependency is increasingly shifting to:

- knowledge structures,
- context models,
- semantic links,
- AI-supported automation
- and platform-bound data spaces.

Modern document formats have long been more than mere file formats. They form the infrastructural basis of digital knowledge work and are increasingly becoming semantic carriers of organisational knowledge.

Today, documents contain not only content, but also:

- comments,
- metadata,
- version histories,
- sharing,
- collaboration information
- and organisational context structures.

AI systems access precisely these structures. Content is no longer merely stored or exchanged, but, by AI systems,

- interpreted,
- prioritised,
- linked
- and processed automatically.

This creates a new form of digital dependency:
it is no longer access to data alone that determines switchability, but control over its semantic interpretation.

7.2 Proprietary AI Ecosystems

Modern AI systems increasingly derive their strength from deep integration into existing platform ecosystems. AI assistants access:

- documents,
- communication,
- calendars,
- meetings,
- permissions,
- knowledge bases
- and organisational processes

and combine this information into context-based work models.[40]

The real value of such systems thus arises less from individual AI models than from exclusive access to integrated data and workflow ecosystems.

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

The more closely AI functions are tied to proprietary platforms, the harder it becomes to migrate organisational knowledge to alternative systems. Digital dependency thus increasingly arises not only through data formats, but through:

- context knowledge,
- semantic links
- and platform-bound knowledge models.

Control over AI ecosystems is thus becoming a new form of infrastructural market power.

7.3 AI Agents and Semantic Dependencies

With the development of autonomous AI agents, this problem intensifies further. AI agents no longer interact only with individual documents, but increasingly with:

- workflows,
- communication systems,
- corporate knowledge
- and organisational processes.

This creates new forms of semantic lock-in effects. Work logic, prioritisation, context models and organisational knowledge structures are gradually mapped into proprietary AI systems.

Migrating such systems becomes considerably more complex than traditional data migration. Even if data remain exportable, this does not automatically mean that:

- context knowledge,
- automations,
- semantic relationships
- or organisational work logic

can be migrated on equal terms.

Specifically, this concerns, among other things, the permissions an assistant may access, links between answers and sources, knowledge graphs, the configuration of agents and the state of running processes. Open standards exist for individual components — for knowledge graphs, for example, the W3C standards RDF and

JSON-LD. For transferring an integrated AI work context as a whole, with permissions, source references, agent configuration and process state, however, there is no established open format.

The actual platform dependency thus increasingly arises at the level of:

- semantic models,
- organisational knowledge structures
- and AI-supported decision logic.

7.4 APIs as the New Standards

In the age of AI, APIs (Application Programming Interfaces) are increasingly becoming the actual standards of digital platform ecosystems. They define[41]:

- how AI systems access data,
- how applications are integrated,
- how automations work
- and which platform services can interact with one another.

Formally open APIs are increasingly no longer sufficient to ensure real switchability. Proprietary extensions, platform-specific SDKs, semantic models and non-standardised integrations create new dependencies that go far beyond traditional file formats.

This becomes particularly relevant for:

- AI agents,
- workflow automation,
- knowledge graphs,
- semantic search systems
- and platform-integrated AI assistants.

Whoever controls the APIs increasingly also controls the semantic infrastructure of digital work.

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

7.5 Risks for European Digital Sovereignty

The next phase of digital sovereignty will therefore not be decided solely by:

- cloud infrastructure,
- data centres
- or data location.

What will increasingly matter is whether:

- knowledge models,
- AI-supported work processes,
- semantic integrations
- and organisational context systems

remain interoperable and migratable in the long term.

A lack of interoperability in AI carries considerable risks:

- increasing organisational dependencies,
- long-term platform lock-in,
- restricted switchability
- and new concentration effects in digital markets.

This is precisely why the question of verifiable interoperability is gaining further importance. The challenges already visible today in document formats, APIs and collaboration platforms threaten to intensify considerably in AI and semantic platforms.

Under these conditions, digital sovereignty means not only control over data, but increasingly also control over:

- semantic structures,
- organisational knowledge
- and AI-supported work processes.

8 Why Open Standards Alone Are Not Enough

The preceding chapters have shown with concrete examples that formal standardisation is not a sufficient condition for practical interoperability. This chapter summarises the structural patterns.

8.1 The Problem of Purely Formal Standardisation

OOXML has been an ISO standard since 2008. Microsoft Office initially did not support the cleaned-up Strict variant and to this day saves by default in the transitional format Transitional, which was not intended for new documents (see Section 3.3). CalDAV (2007) and CardDAV (2011) have been IETF standards for many years; Outlook still does not support them natively (see Section 4.3). IMAP was first specified in 1988; in the new Outlook, it remains functionally restricted compared with Exchange accounts (see Section 4.2).

The pattern is consistent: formal standardisation does not guarantee real interchangeability. Standards deliver their market effect only if they are implemented consistently and interoperable behaviour remains verifiable.

8.2 Missing Compliance Testing

Exchange Web Services was a documented interface on which third-party vendors built for years. Since October 2026 it has been gradually disabled, and from April 2027 it will be shut down permanently; its successor, Microsoft Graph, is a proprietary API without a standardised alternative (see Section 4.4). Whether this switch preserves interoperability for third parties could, under current law, be clarified at most on a case-by-case basis, for example in antitrust proceedings. There is no predefined, publicly traceable review of such interface changes: the DMA's specific interoperability obligations do not apply because Microsoft 365 is not a designated core platform service (see Section 6.4), and the 2025 Teams commitments are a case-specific arrangement whose implementation is monitored by a trustee — not a general, publicly verifiable benchmark.

Compliance testing is missing not only technically – it is missing in regulation.

8.3 Missing Reference Implementations

OOXML Strict exists as a specification. A binding reference implementation showing how Strict is to be implemented correctly does not exist. The result: dominant market implementations de facto define the standard *(see Section 0)*. The same applies to S3-compatible storage services – "compatible" without a reference benchmark is meaningless *(see Section 4.5)*.

8.4 Missing Migratability

Interoperability is often reduced to data export. Actual switchability, however, comprises workflows, permissions, metadata, communication histories and organisational context information *(see Sections 5.3, 5.4 and 5.5)*. In AI-supported systems in particular, the next generation of dependencies arises at the semantic level – not at the file level *(see Chapter 7)*.

8.5 "Open Washing" and Sham Compatibility

The documented examples show a consistent pattern: platforms advertise openness – OOXML as an "open standard", EWS as a "documented interface", S3 as a "compatible protocol" – without this resulting in equivalent usability or real switchability.

This is not necessarily the result of ill intent, and the criticism in this paper does not presuppose such intent. It is directed at the demonstrable mechanism: a market without verifiable conformance mechanisms shifts the costs of deviation onto alternative providers and onto customers who want to switch.

Standards without verifiable conformance are not standards. They are promises.

8.6 Different Problems, Different Answers

The examples in this paper describe related but different problems that require different answers:

- **Document formats:** reliable processing of standardised content between independent implementations;
- **CalDAV and CardDAV:** support for required open interfaces in the first place;
- **IMAP:** the distinction between email functions covered by the standard and calendar functions for which other open standards exist;
- **EWS and Microsoft Graph:** control over the life cycle of interfaces and the adaptation costs borne by third parties;
- **Workflows:** the transferability of organisational routines, permissions and context information.

A product can implement a supported protocol correctly and at the same time not offer important open interfaces at all. A pure conformance test would therefore not be enough. Both are needed: binding minimum requirements specifying which open interfaces a service must support, and tests of whether it implements them reliably.

9 Proposal: A European Interoperability Certification

9.1 Basic Idea and Objectives

The preceding chapters show a structural problem of digital markets: open standards alone are not enough to ensure real interchangeability and functioning competition. What matters is not only the existence of a standard, but its verifiable interoperable implementation.

This is exactly where the proposal for a European interoperability certification comes in.

The aim of such a system would not be to regulate technological innovation, to disadvantage individual platforms — or to establish technological autarky. Rather, the aim would be to create verifiable market transparency:

- Which systems actually implement standards interoperably?
- Which platforms enable real switchability?
- Which solutions create long-term structural dependencies?

A European interoperability certification would thus fulfil a function similar to technical certification in traditional industries:
it would not prevent innovation, but create trust, interchangeability and market transparency.

9.2 An Independent European Certification Body

A precondition for a credible interoperability certification system would be an independent European governance and testing framework.

The task of such a structure would not be to favour individual technologies or providers, but to ensure the objective verification of practical interoperability on the basis of transparent technical criteria.

A suitable model would be a decentralised network of nationally accredited testing bodies under a common European framework – comparable to existing conformity and certification systems in other industrial sectors.

Europe already has numerous institutional structures that could serve as an organisational basis for this. These include in particular:

- national standardisation and certification organisations such as Austrian Standards (Austria), DIN (Germany) and AFNOR (France),
- the European standardisation organisations CEN, CENELEC and ETSI,
- specialised agencies such as ENISA in the field of European cybersecurity certification
- and existing national IT certification bodies such as the German Federal Office for Information Security (BSI).

No entirely new institutional system would therefore have to be created. Rather, an interoperable European certification framework could build on existing standardisation, testing and accreditation structures.

Institutional independence would be decisive here:
certification would have to be

- transparent,
- traceable,
- reproducible
- and vendor-neutral.

Only in this way can the necessary trust arise – among companies, public institutions and alternative providers alike.

9.3 Technical Compliance Tests

A core component of an interoperability certification would be standardised technical compliance tests.

The question would be not only whether a standard has been formally implemented, but whether different systems work interoperably in practice.

Such tests could, for example, examine:

- consistent document rendering,
- lossless migration,
- interoperable calendar and contact synchronisation,
- API compatibility,
- workflow behaviour,
- permission models
- or cross-platform collaboration features.

The practical user perspective would be particularly relevant here: interoperability must prove itself not only in theory, but in real-world use.

In complex platform ecosystems in particular, mere conformance with a specification is often not enough to ensure real interchangeability.

9.4 Reference Implementations and Test Suites

Technical standards require verifiable reference models. A European interoperability certification should therefore be supplemented by:

- open reference implementations,
- standardised test suites
- and publicly documented conformance criteria.

The aim would be to reduce scope for interpretation and asymmetric implementations.

The basis should be a publicly accessible test corpus. Each test case should document at least:

- **Source document:** the function used and the format profile claimed;
- **Test environment:** products, versions and relevant settings;
- **Expected behaviour:** the basis in the specification or test profile;
- **Actual behaviour:** the reproducible deviation;
- **Editing cycle:** not only opening, but also editing and saving in the alternative product and reopening in the original product;
- **Classification:** breach of the standard, gap in the specification, vendor extension or implementation error;
- **Consequence for the customer:** loss of information, rework or obstacle to switching.

Influencing factors such as missing fonts must be controlled for; not every layout error is a breach of the standard. It is precisely this care that makes the findings robust: structural problems can then not be dismissed as mere bugs in competing programs, and the classification shows whether the implementation must be corrected, the standard made more precise or an interoperability profile added.

Particularly in the area of:

- document formats,
- APIs,
- collaboration platforms
- and AI-supported workflow systems,

such reference models could contribute considerably to practical interoperability.

The reference implementation itself would become neither a mandatory market standard nor an unassailable benchmark. The published requirements remain authoritative; the reference implementation is a tool for testing against them.

This would avoid the situation common today in which dominant market implementations de facto themselves become the reference standard.

9.5 Certification Levels, Enforcement and Funding

Not every form of interoperability has the same level of maturity. A tiered certification model therefore appears sensible. A certificate should not assure “interoperability” across the board, but compliance with a binding, versioned test

profile with defined functions, permissible tolerances and clear pass criteria. Within a profile, the requirement must remain strict: a material incompatibility cannot be offset by predominant conformance. To avoid confusion with CADA assurance levels 1 to 4, the certification levels are designated here by Roman numerals.

Level I – Verified Baseline Profile

It has been independently verified that the service complies with a binding baseline profile — the open standards and basic functions that are required as a minimum for the type of service concerned. The provider also documents deviations and vendor-specific extensions. This disclosure is mandatory, but does not legitimise a breach of the baseline profile: a provider that does not meet the baseline profile does not receive the certificate, even if it discloses the deviation.

This does not yet guarantee full practical interchangeability, but it creates market transparency as a basis for informed procurement and architecture decisions.

Level II – Verified Interoperability

For the functions of a versioned test profile, tests with independent implementations have demonstrated that they are processed consistently within the specified tolerances.

Test profiles can cover, for example, document rendering, calendar and contact synchronisation, metadata, comments and versions, or cross-platform collaboration.

Level III – Verified Switchability

The highest level confirms, in a standardised reference scenario, that data, documents, metadata, permissions and defined workflows can be migrated to an independent implementation. Besides the functionality retained, the evidence also documents the effort, costs, duration of parallel operation and of service interruption, and remaining dependencies.

A technically possible migration is not an adequate switching option if it requires disproportionate costs, months of parallel operation or extensive manual reconstruction. This is not a demand for a free or effortless change of provider,

but the necessary distinction between theoretical exportability and an option for action that can actually be carried out.

The following applies to all levels:

- test criteria and results are publicly accessible;
- relevant product changes trigger a new test;
- identified deficiencies must be remedied within a deadline;
- in the event of non-compliance, the certificate is suspended or withdrawn.

Enforcement and Economic Relevance

Certification levels take effect only if they become economically and regulatorily relevant.

Four mechanisms in particular appear suitable for this:

Public procurement: Award procedures of public institutions could gradually define interoperability-related minimum requirements. For example, at least Level I could be required for general workplace systems, and at least Level II for systems subject to long-term archiving obligations or particularly critical systems. This corresponds to the established principle of technical proof of conformity in other industrial sectors: it is not the provider that is regulated, but the interoperable property of the product that is demonstrated transparently.

Integration into existing DMA interoperability mechanisms: For platform providers with particularly strong market power, interoperability certifications could in future be linked more closely to existing regulatory instruments – for instance in the context of the Digital Markets Act. This would be particularly relevant where platform ecosystems create considerable switching costs, organisational dependencies arise or asymmetric interoperability creates structural market advantages.

Transparency obligation: Providers of digital workplace, collaboration and platform solutions could be required to disclose their interoperability status transparently. A lack of certification would not be a sales ban – but it would create market transparency about migratability, conformance with standards and practical interchangeability.

Linkage to the CADA: In the medium term, the CADA assurance levels could be tied to proof of interoperability — for example, such that services at CADA levels 2 to 4 require at least Level II certification and services at level 4 additionally require proof of switchability under Level III. The highest assurance level in particular should not be attainable without tested replaceability. This would examine not only how exposed a service is to third countries, but also whether it can be replaced.

Funding

The certification system should be financed primarily through certification fees – analogous to existing conformity and testing procedures in other industrial sectors.

It is particularly important that interoperability certification must not itself become a barrier to market entry. Reduced fee models should therefore be provided for open-source projects, small and medium-sized providers and public-interest digital infrastructure projects.

The development of open test suites, reference implementations and interoperable testing tools could additionally be co-financed by European research and innovation programmes.

Timetable

The specific timetable for introduction is a matter for political agreement between the European Commission, the Member States and standardisation organisations. As a frame of reference, the following phasing appears realistic:

- *Phase 1 (years 1–2)*: establishment of the certification framework, development of open test suites and pilot operation with voluntary certification
- *Phase 2 (years 3–4)*: mandatory Level I procurement requirement for the public sector
- *Phase 3 (from year 5)*: mandatory Level II requirement for security-critical systems and systems subject to archiving obligations, and linkage with the CADA and with DMA mechanisms for providers with market power

9.6 Interoperability as Market Transparency

A European interoperability certification would not only make technical quality visible, but above all create structural market transparency.

Companies and public bodies could thus better assess:

- which platforms enable real switchability,
- which systems create long-term dependencies
- and which solutions remain interoperable and migratable.

Interoperability would thus turn from a technical detail that is hard to verify into a visible competitive feature.

This is where the real economic-policy significance of such a system lies: not regulation for its own sake, but the creation of transparent preconditions for functioning digital markets.

9.7 Proportionality, Openness and Low Barriers to Entry

A European interoperability certification can deliver its economic-policy effect only if it does not itself create a new barrier to market entry.

Certification procedures must therefore be designed to be:

- transparent,
- reproducible,
- modular
- and as automatable as possible.

For small and medium-sized European providers in particular, a highly complex or costly certification system would be problematic. Interoperability regulation must not unintentionally reinforce existing market concentration.

Dominant platform providers in particular have considerable organisational and financial resources to cope with complex compliance and certification processes. Small providers, open-source projects and specialised European providers often do not have these capabilities to the same extent.

A functioning certification model must therefore deliberately create low barriers to entry.

These include in particular:

- open and publicly documented test suites,
- standardised reference tests,
- reproducible testing procedures,
- modular certification components
- and largely automatable conformance tests.

Certification should not rely solely on elaborate individual audits, but should build as far as possible on:

- open technical tests,
- standardised validation procedures
- and transparent conformance criteria.

A tiered model appears sensible here:
simple implementations of standards should be certifiable with little effort, while complex platform ecosystems must provide correspondingly more extensive proof of interoperability.

It is particularly important that
the actual reference must not be defined by individual dominant market implementations, but by open, traceable and reproducible technical criteria.

Interoperability certification must not itself become a lock-in. Its aim must be to lower barriers to switching – not to create new regulatory dependencies.

10 Public Procurement as a Strategic Lever

10.1 The Public Sector as a Market Shaper

The public sector is one of the largest buyers of digital technologies in Europe. Public administrations, educational institutions, health systems and state-affiliated organisations invest billions every year in:

- software,
- cloud services,
- collaboration platforms
- and digital infrastructure.

Procurement is thus not merely an operational administrative function, but a central lever of economic policy. Public tenders influence:

- technological standards,
- market structures,
- the dynamics of innovation
- and long-term platform dependencies.

In the digital sphere in particular, this has considerable structural effects. When public institutions procure platform ecosystems that are only partly interoperable or migratable, they reinforce existing lock-in structures in the long term.

Digital sovereignty is therefore not solely a question of technological development, but also a question of strategic procurement policy.

10.2 Certification as a Procurement Requirement

Interoperability takes effect only if it becomes economically relevant. This is precisely where public procurement can play a central role.

A European interoperability certification could gradually be established as an objective evaluation criterion in public tenders. The aim would not be to exclude individual providers, but to create transparent requirements for:

- switchability,
- data migration,
- conformance with standards
- and practical interoperability.

Interoperability would thus become comparable systematically, in a publicly traceable way and with effect in procurement.

This would be particularly relevant in areas with long-term dependencies:

- document management,
- collaboration platforms,
- cloud services,
- communication systems
- and AI-supported work environments.

Procurement decisions would then no longer assess only short-term functionality, but also take account of long-term digital resilience and migratability.

The timing is favourable: on 9 September 2026, the Commission proposed replacing the 2014 procurement directives with a directly applicable regulation that provides, among other things, for a framework for European preferences and a common digital procurement infrastructure.[42] The negotiations in the European Parliament and the Council offer an opportunity to anchor verifiable interoperability and tested switchability as a selection or award criterion for digital workplace and collaboration systems.

10.3 Promoting Competition and Innovation

Interoperability strengthens competition. When switching costs fall and platforms remain interchangeable in practice, the result is:

- lower barriers to market entry,
- greater room for innovation
- and more competition between different providers.

European providers in particular could benefit. Today, many digital markets impose considerable structural disadvantages through:

[42] Proposal for a Regulation on public procurement and concessions, COM(2026) 590 final of 9 September 2026.

- dominant platform ecosystems,
- proprietary integrations
- and asymmetric interoperability.

Small and medium-sized providers often have to implement not only open standards, but also replicate the behaviour of dominant platforms in order to remain competitive.

Binding interoperable standards and verifiable conformance mechanisms could reduce these structural disadvantages.

Interoperability thus becomes not an obstacle to innovation, but a precondition for functioning innovation markets.

10.4 Opportunities for European Providers

Europe has numerous capable providers in areas such as:

- cloud infrastructure,
- open-source software,
- collaboration platforms,
- security solutions
- and digital administration systems.

Many of these providers, however, fail not because of a lack of technical quality, but because of:

- high switching costs of existing platform ecosystems,
- asymmetric interoperability
- and a lack of practical interchangeability.

A procurement framework oriented towards interoperability could create new market opportunities here. Public institutions would not primarily favour individual technologies, but systems that:

- implement open standards interoperably in practice,
- enable real switchability
- and reduce long-term platform dependencies.

European providers could thus compete more on:

- quality,
- security,
- innovation
- and service

– rather than primarily against existing lock-in structures.

10.5 Long-Term Archiving and Sustainability

Public procurement concerns not only current product decisions, but often digital infrastructures with a lifespan of decades.

Documents, administrative data, scientific information and organisational knowledge must remain, in the long term:

- readable,
- migratable
- and usable independently of individual platform ecosystems.

A lack of interoperability creates considerable risks here:

- rising migration costs,
- long-term vendor dependencies,
- loss of semantic information
- or restricted archivability.

In the public sector in particular, this creates a conflict of objectives between short-term functionality and long-term digital resilience.

Under these conditions, interoperability becomes a question of sustainable public infrastructure policy.

The public sector therefore has not only the opportunity but also the responsibility to actively promote interoperable and migratable digital systems.

Public procurement can thus become a central instrument for structurally strengthening:

- competition,
- digital sovereignty
- and long-term technological resilience.

11 Recommendations

The preceding chapters have shown that digital sovereignty cannot be achieved through European infrastructure or formal standardisation alone. What matters is whether digital systems remain interoperable, migratable and interchangeable in practice in the long term.

The specific proposals are set out in Chapters 9 and 10. This chapter addresses the central recommendations explicitly to the relevant addressees.

Preliminary Note on Terminology

Microsoft Office refers to the most widely used office software suite in European companies and public institutions – consisting of Word, Excel, PowerPoint and Outlook. It is distributed both as a perpetual licence (Microsoft Office 2024) and as a cloud subscription under the name Microsoft 365 – with or without the AI extension Copilot. The market power of Microsoft Office exists regardless of the form of licensing and regardless of product-related renaming. In the context of this paper, "Microsoft Office" refers to the product in all its forms of distribution.

Microsoft Office dominates the market for office software in European companies and public bodies. An analysis by Compass Lexecon commissioned by the Open Cloud Coalition estimates Microsoft's share of the market for productivity software in the EU public sector at around 77%, and in the segment of office applications at up to 90%.[43] Google Workspace follows at a considerable distance. All other providers — including LibreOffice, OnlyOffice and other European solutions — share the remainder.

High market shares are not problematic in themselves.

Functioning markets presuppose real switchability.
When platform ecosystems are barely interchangeable in practice any more because of proprietary integrations, workflow dependencies and semantic ties, competition loses its disciplining effect.

[43] Compass Lexecon (2025): Quantifying EU public sector dependence on productivity software, commissioned by the Open Cloud Coalition. The figures are estimates based on commercial market data and public procurement data; the client is an interest group. On the combined share of Microsoft and Google in collaboration software, see Illsinger, W. (2026): Digital Sovereignty in Europe. Definition, Status, Policy Options. Policy Brief No. 2026-001 (EN), Version 3. Vienna: 4future.institute. DOI: 10.5281/zenodo.24042486. Section 2.2.

11.1 To the European Commission

Extend the Digital Markets Act with binding interoperability requirements for:

- **digital work and collaboration platforms –** in particular for document formats, calendar and contact protocols, programmatic interfaces and interoperability between services
- **cloud infrastructure standards and APIs –** in particular where proprietary interfaces have become de facto market standards without a regulatory basis
- **AI platform ecosystems and semantic knowledge systems –** in particular where proprietary AI agents and knowledge models create new forms of migration-induced platform lock-in

Examine whether Microsoft Office — distributed as a perpetual licence and as a cloud subscription under the name Microsoft 365 — can be covered as a core platform service and Microsoft designated as a gatekeeper for it: as a cloud computing service in its form as Microsoft 365 or, if necessary, by adding to the list of core platform services. Such an addition can be prepared by a market investigation under Art. 19 DMA; it would have to be adopted by the legislator. Microsoft is already designated as a gatekeeper for other services; the lock-in effects through asymmetric interoperability documented in Chapter 4 correspond to the protective purpose of the DMA. The ongoing market investigation into the application of the DMA to cloud services should expressly also include office and collaboration services offered as software as a service.

Examine gatekeeper designation for further platforms that have not yet been designated despite meeting the DMA's quantitative thresholds – in particular where de facto standards have emerged without a regulatory basis or migration-induced platform lock-in structurally prevents switching.

Issue a standardisation request under Regulation (EU) No 1025/2012 to CEN, CENELEC and ETSI for the development of a European interoperability certification framework based on existing standardisation and accreditation structures — involving the Interoperable Europe Board and drawing on ENISA's experience with the European cybersecurity certification framework.

Introduce a binding transparency obligation for providers of digital workplace and collaboration solutions regarding their interoperability status – as a basis for informed procurement decisions by public and private institutions.

Link the CADA assurance levels to proof of interoperability in the negotiations on COM(2026) 502 — with documented data portability, open formats and a tested exit plan at every level.

Anchor verifiable interoperability and tested switchability as a selection or award criterion in the proposed procurement regulation COM(2026) 590.

Publish the results of the trustee's monitoring of the Teams commitments in a form that allows third parties to verify the promised interoperability.

11.2 To the Austrian Federal Government and EU Member States

Introduce interoperability certification as a procurement requirement for public contracts for digital workplace and collaboration systems – gradually, starting with Level I certification.

Commission Austrian Standards International to develop a national pilot programme for interoperability certification – as a basis for a European certification framework.

Promote open reference implementations and test suites within national digital programmes – in particular for IMAP, CalDAV, CardDAV, ODF and OOXML Strict.

Actively raise the issue of verifiable interoperability in European digital policy — in particular in the implementation of the Interoperable Europe Act and in the negotiations on the CADA and the procurement regulation.

11.3 To Standards Bodies and Standardisation Organisations

Develop standardised compliance tests for open protocols – IMAP, CalDAV, CardDAV, ODF, OOXML Strict – as publicly accessible test suites.

Build a European network of accredited interoperability testing bodies under a common framework – analogous to existing conformity assessment systems.

Participate actively in the further development of the Interoperable Europe Act and in European standardisation processes for digital workplace and collaboration systems.

Develop a tiered certification model with low barriers to entry – in particular for open-source projects and small providers.

11.4 To Civil Society and Academia

Systematically document and publish interoperability deficiencies in real work environments – as a basis for evidence-based regulation.

Build open test suites and reference implementations as digital commons – funded by European research and innovation programmes such as Horizon Europe.

Provide independent academic oversight of the certification process – to ensure technical neutrality and vendor independence.

12 Conclusion

In recent years, the European debate on digital sovereignty has focused above all on:

- infrastructure,
- cloud platforms,
- data protection
- and geopolitical dependencies.

This perspective remains important. But it falls short.

Today, digital dependency increasingly arises not only at the level of data centres or data locations, but within digital work and knowledge ecosystems:

- in document formats,
- APIs,
- collaboration platforms,
- workflow systems
- and semantic AI structures.

It is precisely there that it is decided whether digital systems remain, in the long term:

- interoperable,
- migratable
- and interchangeable in practice.

The central finding of this paper is therefore:

Open standards alone are not enough.

Standards deliver their economic and social effect only if:

- their implementation remains interoperable,
- their conformance is verifiable
- and real switchability between platforms remains possible.

Without this practical interoperability, despite formal openness, the result is:

- high switching costs,
- structural lock-in effects
- and long-term market concentration.

The consequence is a creeping shift of digital power:
away from open markets,
towards integrated platform ecosystems.

This development becomes particularly critical in the age of AI-supported knowledge systems. The next generation of digital dependency no longer arises only through documents or data formats, but increasingly through:

- semantic models,
- organisational knowledge,
- APIs,
- AI agents
- and platform-bound context systems.

Under these conditions, digital sovereignty means not only control over infrastructure or data location. It increasingly also means:
the ability to switch digital systems in practice.

Interoperability thus becomes a central precondition for:

- functioning digital markets,
- technological resilience,
- long-term capacity for innovation
- and Europe's capacity to act.

In this area, Europe has the opportunity to develop its own regulatory and technological path. The Digital Markets Act has begun to address structural platform power and, with the proceedings on AWS and Azure, is being extended to cloud infrastructure for the first time; the Teams commitments, the Data Act and the Interoperable Europe Act add further pieces. The question of verifiable interoperability of digital work and knowledge ecosystems, however, remains largely unresolved.

This paper therefore proposes:

- to verify interoperable standards more rigorously in practice,
- to establish European certification models,
- to promote open reference implementations
- and to integrate interoperability systematically into public procurement.

The aim is not to restrict technological innovation.

On the contrary:
open and verifiably interoperable systems create the foundation for:

- competition,
- innovation,
- market diversity
- and long-term digital resilience.

Interoperability is thus not a technical side issue. It is becoming one of the central industrial, economic and social policy challenges of digital societies.

In future, the decisive question will no longer be only:

> "Are standards open?"

But:

> "Do they enable real digital freedom?"

Standards without verifiable conformance are not standards. They are promises.

I. About the Author

Ing. Werner Illsinger, MBA, is founder and Executive Director of the 4future.institute. He worked for Microsoft for 18 years — from the era of the personal computer to the age of cloud dominance. He witnessed how a company that once democratised the PC became a global platform infrastructure that today controls central functions of society — and draws conclusions from this for Europe.

Trained as a communications engineer and business psychologist, he combines a technical understanding of systems with a systemic and societal perspective. This paper was not commissioned — it is the result of a growing conviction that Europe must shape the structural conditions of its digital future now, while the window is still open.

II. Annex: Definitions

AI agent

An AI agent is a software-based system that can carry out tasks, prepare decisions or control work processes autonomously or semi-autonomously.

AI agents often access

- documents,
- APIs,
- communication systems,
- calendars
- and knowledge models.

API (Application Programming Interface)

An API is a defined interface through which different software systems can communicate with one another. APIs specify how applications exchange data or use functions of other systems.

In the context of the digital platform economy, APIs are increasingly becoming strategic control points of digital ecosystems.

Asymmetric interoperability

Asymmetric interoperability describes a situation in which systems work with one another in principle, but not on equal terms.

The dominant platform typically offers:

- the greatest functional scope,
- the greatest depth of integration,
- the most consistent user experience
- and the lowest risks.

Alternative providers remain formally compatible, but often bear higher interoperability and reputational risks.

CalDAV

CalDAV is an open standard for synchronising calendar data between different systems.

CalDAV enables, among other things:

- shared calendars,
- appointment management,
- invitations
- and cross-platform synchronisation.

CardDAV

CardDAV is an open standard for synchronising contact and address book data.

The standard enables the interoperable exchange of contact data between different platforms and applications.

Collaboration platform

A collaboration platform is an integrated digital work environment for:

- communication,
- document editing,
- meetings,
- workflow control,
- task management
- and collaboration.

Examples include platforms such as Microsoft Teams, SharePoint or comparable work ecosystems.

Compliance test

A compliance test verifies whether a technical standard has actually been implemented correctly and interoperably.

In contrast to purely formal support for a standard, a compliance test assesses the practical behaviour of a system.

Data portability

Data portability refers to the possibility of exporting data from one system and transferring it to another system.

Data portability alone, however, does not yet guarantee full switchability or interoperability.

De facto standard

A de facto standard is a standard that has become established in practice through market adoption, regardless of whether it has been officially standardised.

Dominant platform implementations often develop into de facto standards.

Digital Markets Act (DMA)

The Digital Markets Act is a European regulation to limit the structural market power of large digital platform providers ("gatekeepers").

The DMA contains, among other things, requirements on:

- interoperability,
- data portability,
- opening of platforms
- and competitive conduct.

Digital sovereignty

Digital sovereignty refers to the ability of states, organisations and individuals to use digital technologies independently, in a controllable way and while retaining their capacity to act in the long term.

This includes, among other things:

- control over infrastructure,
- data sovereignty,
- switchability of digital systems,
- interoperability
- and technological resilience.

Functional equivalence

A term of the Data Act (Art. 2(37)): after switching providers, a service of the same type delivers, with the same input, materially comparable outcomes for the shared functions. The Data Act requires support for functional equivalence only from providers of infrastructure services (IaaS).

Gatekeeper

Gatekeepers are particularly large digital platform providers with structural market power.

The term is used in particular in the Digital Markets Act.

Gatekeepers often control central digital gateways or platform ecosystems.

IMAP

IMAP (Internet Message Access Protocol) is an open standard for accessing email mailboxes.

IMAP enables the synchronisation of email between different devices and mail servers.

Interchangeability

Interchangeability refers to the practical possibility of switching digital systems or platforms without disproportionate technical, economic or organisational hurdles.

Interchangeability comprises more than the mere ability to export data. What matters is whether:

- documents,
- workflows,
- metadata,
- organisational routines
- and semantic structures

remain migratable in practice.

Interoperability

Interoperability refers to the ability of different systems, applications or platforms to work together consistently and interchangeably.

Practical interoperability means that defined functions work consistently in specified use cases between independent implementations within agreed tolerances — including the full editing cycle.

Interoperable Europe Act

Regulation (EU) 2024/903 laying down measures for a high level of public sector interoperability across the Union. Among other things, it requires public bodies to carry out interoperability assessments before establishing binding requirements for trans-European digital public services.

ISO standard

An ISO standard is an internationally standardised technical standard of the International Organization for Standardization (ISO).

ISO standards define common technical specifications and are intended to promote interoperability and interchangeability.

Lock-in effect

A lock-in effect describes a situation in which switching a system or platform provider involves high technical, organisational or economic costs.

Lock-in often arises from:

- proprietary extensions,
- a lack of interoperability,
- workflow dependencies
- or network effects.

Metadata

Metadata are structured additional information about data or documents.

Examples include:

- author information,
- version histories,
- sharing settings,
- timestamps
- or permissions.

Network effect

A network effect arises when the benefit of a system increases with the number of its users.

Digital platform markets often exhibit strong network effects.

ODF (OpenDocument Format)

ODF is an open, ISO-standardised document format for texts, spreadsheets and presentations.

ODF was developed to enable long-term vendor independence and interoperable document formats.

OOXML (Office Open XML)

OOXML is an XML-based document format for office documents.

OOXML was developed by Microsoft and standardised as an ISO/IEC standard in 2008.

The standard exists in the variants “Strict” and “Transitional”.

Platform economy

The platform economy describes digital markets in which platform providers act as central intermediaries between different market participants.

Platforms often benefit from:

- network effects,
- integration advantages,
- data aggregation
- and lock-in effects.

Proprietary extension

A proprietary extension adds functions to an open standard that are fully supported only within a particular platform ecosystem.

Formal openness can thus remain while practical interchangeability is restricted.

Reference implementation

A reference implementation is a technical implementation of a standard that serves as an objective benchmark for comparison.

Reference implementations help:

- to reduce scope for interpretation,
- to test interoperability
- and to make conformance verifiable.

S3 (Simple Storage Service)

S3 is a cloud storage service developed by Amazon for object-based data storage.

In recent years, the S3 API has in effect become the de facto standard for object-based cloud storage solutions.

Many providers therefore advertise “S3 compatibility”.

Semantic platform

A semantic platform not only processes data, but interprets their meaning, context and relationships.

Such platforms play a central role, particularly in AI-supported knowledge systems.

Standard

A standard defines common technical rules or specifications in order to enable interoperability, interchangeability and compatibility between different systems.

Standardisation

Standardisation refers to the process of defining and harmonising technical rules or formats.

Standardisation alone, however, does not yet guarantee practical interoperability.

Workflow lock-in

Workflow lock-in describes a form of digital dependency in which organisational routines, automations and process logic are closely tied to a particular platform ecosystem.

The actual barrier to switching arises less from data formats than from integrated work processes.

III. Annex: Sources & Literature

EU Legislation and Legislative Proposals

Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act).

Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act).

Regulation (EU) 2024/903 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act).

Directive (EU) 2022/2555 (NIS 2 Directive).

Directive (EU) 2022/2380 (common charger).

Regulation (EU) No 1025/2012 on European standardisation.

European Commission (2026): Proposal for a Cloud and AI Development Act, COM(2026) 502 final, 3 June 2026.

European Commission (2026): Proposal for a Regulation on public procurement and concessions, COM(2026) 590 final, 9 September 2026.

European Commission (2017): European Interoperability Framework – Implementation Strategy (new EIF), COM(2017) 134.

Decisions and Proceedings of the European Commission

Designation decision on Microsoft under the DMA of 5 September 2023; Decision C(2024) 806 of 12 February 2024 (Bing, Edge, Microsoft Advertising), OJ C/2024/2709.

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

Market investigations into cloud computing services under the DMA, 18 November 2025; preliminary position on AWS and Microsoft Azure, 25 June 2026 (IP/26/1444).

Standards and Specifications

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.

Company Documentation and Documentation on Document Standards

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

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

Microsoft Support: Feature comparison between new Outlook and classic Outlook (continuously updated).

Microsoft Q&A: questions 5742426 (27 January 2026) and 5853986, answers from 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 March 2010.

Commonwealth of Massachusetts, Information Technology Division: Enterprise Technical Reference Model, Version 3.5 (2005) and 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 project of Generalize-IT Solutions OG, Vienna, https://github.com/aluxnimm/outlookcaldavsynchronizer.

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

SmarterTools (2017): Microsoft Outlook 2016 and EAS, 4 October 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: bugs 160518 (2024) and 134509 (2020); Collabora Online forum, thread 4664 (2026).

Market Data

Compass Lexecon (2025): Quantifying EU public sector dependence on productivity software. Commissioned by the Open Cloud Coalition.

Microsoft (2023): Results for the first quarter of fiscal year 2024, 24 October 2023.

Academic Literature

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

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

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

Publications of the 4future.institute

Illsinger, W. (2026): Digital Sovereignty in Europe. Definition, Status, Policy Options. Policy Brief No. 2026-001 (EN), Version 3. Vienna: 4future.institute. DOI: 10.5281/zenodo.24042486. German original: Digitale Souveränität in Europa. Definition, Status, Handlungsoptionen. Policy Brief Nr. 2026-001 (DE). DOI: 10.5281/zenodo.24042085.

4future.institute (2026): Strategie für eine lebenswerte Zukunft. 4future.institute Papers No. 2026-001, ISSN 3061-1903 (in German).



Society. Economy. Technology. Sustainability.

The future emerges from balance and conscious design.

The 4future.institute is part of the 4future.group and is organised as an independent unit within 4future business GmbH. Its majority shareholder is the 4future.foundation.

Independence is the precondition of our work — not its result

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