RESEARCH & INNOVATION

CII WHITE PAPER

Between quasi-monopoly and sovereignty washing:

Obstacles to a sovereign cloud infrastructure for the German administration

Michael Kolain, *Senior Fellow at the cyberintelligence.institute*

CYBER|INTELLIGENCE
.Institute

Contents

The author

Michael Kolain, Senior Fellow

Michael Kolain is a fully qualified lawyer and expert in digital policy. At FÖV Speyer, he worked with Prof. Mario Martini's team to establish the "Digitalization" program area and conducted research on AI regulation, digitalization of administration, and data (protection) law. As a parliamentary advisor on digital policy, he contributed to the legislation of the „traffic light coalition" government. He works at the interface between legislation, science, and the development of digital technologies.

Executive Summary

Public administration in Germany is effectively dependent on Microsoft in central areas of its IT. With closed ecosystems, targeted product bundling, restrictive license management and massive lobbying, the company has built up a quasi-monopoly position. This systematically stands in the way of open, free and fair competition in the European cloud market.

The consequences are limited freedom of choice, growing security risks, a lack of transparency and dwindling budgetary sovereignty in public budgets. Lock-in effects act as leverage: proprietary standards, the close integration of client, server and cloud as well as high migration costs to alternative solutions, keeping public authorities in the Microsoft ecosystem. Digitally sovereign alternatives stand virtually no chance despite the wide range of offerings available. At the same time, the announced move away from perpetual on-premise licenses and the transition to mandatory subscription models with an Azure connection from 2029 will exacerbate dependency. Prices and conditions are moving into Microsoft‘s sphere of influence - including currency and escalation risks.

> **These accumulating factors are toxic for the digital sovereignty of public administration. The state loses control over code, update policy and data flows.**

These accumulating factors are toxic for the digital sovereignty of public administration. The state loses control over code, update policy and data flows. This is because Microsoft shields central components, such as trade secrets, and rolls out global updates that can neither be comprehensively audited in advance nor sufficiently customised to meet the needs of German authorities. Security incidents in recent years - from supply chain disasters to data breaches - have shown how vulnerable a centralised cloud model can be: any weakness in the core radiates to the periphery and makes the state potentially vulnerable. There are legal and compliance uncertainties to consider as well, such as non-transparent processing of diagnostic data, extraterritorial *data dominance* and limited ability to check what exactly happens when systems are accessed remotely for maintenance. Even seemingly sovereign operating models do little to change this: partially sovereign design variants with national data centres or “EU data borders” address symptoms, not causes.

> **As long as code, updates and architecture control are located within a single company, legal and technical de-pendencies remain.**

As long as code, updates and architecture control are located within a single company, legal and technical dependencies remain – even if higher prices for such “security shells” without real independence will worsen cost control.

In terms of competition policy, Microsoft is shifting market logic through strategic bundling of individual products and closely interwoven sales networks. For example, the Teams communication tool is included but interfaces are not sufficiently open, so interoperable alternatives lose their traction. Decades of lobbying, dense partner structures and multi-year framework agreements consolidate dominance, making it difficult for public procurers to anchor manufacturer-independent, modular architectures in the digital machine room. This creates a vicious circle: politicians react to short-term operational capability; the market adapts to dominance and then the state’s strategic ability to control its IT working environment in a self-determined manner decreases.

This situation is not compatible with the political goal of digital sovereignty. After all, digital sovereignty requires genuine freedom of choice - technically, legally and economically. The cycle of the BMI framework agreement with Microsoft (now running until 2028 and the formational basis for most procurement processes at federal, state and local level) should be used as a transition phase to plan and implement a gradual move away from monolithic IT dependencies. This includes the binding anchoring of open standards and interfaces in future contracts (portability, interoperability, exit rules), cross-vendor reference architectures with clear workload criteria instead of cloud compulsion, mandatory audits with code insight under confidentiality, unchangeable and continuously verifiable logging of all remote access, key sovereignty with the authorities as well as reliable cost and dependency balances across all administrative levels. The German state itself must take the lead instead of being enticed by promises of -

> **The German state itself must take the lead instead of being enticed by promises of - as the German Informatics Society puts it - "sovereignty washing".**

as the *German Informatics Society* puts it - "sovereignty washing". Antitrust investigations should examine in detail all licensing and bundling practices that effectively undermine freedom of choice and address them with appropriate regulatory measures. At the same time, the EU member states are called upon to promote European and open alternatives in a targeted manner - through consortia, reference implementations and a coordinated EU procurement strategy that positions Germany as an anchor customer and endorses the negotiating power of the public sector across national borders. France and Germany should use the "Digital Sovereignty 2025 Summit" on November 18, 2025 to set the decisive course for a sovereign administrative cloud worthy of the name.

The public sector must lead by example. This entails actively and immediately reducing existing dependencies on Microsoft, setting up pilot and migration paths for open, interoperable solutions, finance skills development and focusing strictly on procuring modular solutions. Digital sovereignty is not a PR label, but a government mandate. It is created through political leadership, technical implementation and competitive enforcement. Those who consistently rely on open ecosystems today will reduce security and supply chain risks tomorrow, strengthen budgetary sovereignty and create a resilient IT basis that is sustainable across Europe. After all, only a state that controls and sovereignly manages its own work bases, infrastructures and communication processes is resilient to external threats.

Chapter 1:
Introduction

If you go into a German office, you will not just find piles of files, paper clips and stamps on the desks, but also - as with most German offices - computers. Even if it seems different from the perspective of citizens, who often still have to communicate with governmental departments by post, the work routines of the public sector have largely been technologically connected in recent decades. Without hardware and software, most authorities would not be able to work today. However, the increase in digital equipment has led to intensive business relationships with private IT service providers. At the software level, the Microsoft Group dominates digital administration.

Any public administration employee booting up a government computer will generally see the Windows operating system logo. Anyone preparing an administrative act or writing memos will use Microsoft's Office suite: *Word* for texts, *Excel* for spreadsheets and *PowerPoint* for presentations. Almost every job advertisement in the public sector requires confidence in using Microsoft applications. Yet when it comes to equipping the administration and its ability to work, it should be out of the question - the only exception to this, a transitional period - to justify dependencies on a single provider. For example, it is perfectly natural for the German administration to purchase printer paper, desks, laptops and filing cabinets from different producers with the best price and offer in each case. This means that the state remains independent of individual suppliers and can always keep its procurement routines flexible. However, almost every budget of local authorities, federal states and ministries have a considerable amount of Microsoft licenses on the debit side of their budgets, with the prospect of using alternative providers and competitors left in a neglected corner.

The fact that the administration is drip-fed by a corporation which, according to the Federal Cartel Office, has an "outstanding cross-market significance for competition", can come into conflict with the constitutional requirement that the administration must carry out its tasks independently and in accordance with legal requirements.

What could the German government do if Microsoft stubbornly refuses to renegotiate the BMI framework agreement and simply doubles or trebles its prices? Ultimately, the answer to this question is all the more relevant if a single company, Microsoft, essentially holds and maintains a monopoly on productivity software from the cloud in Germany, thereby deliberately hindering the switch to alternative providers in a free, open and interoperable market.

> **Despite the geopolitical upheavals, Germany is on the verge of deepening its cooperation with Microsoft in 2025, even though the US company is pursuing a business policy that aims to make the state even more dependent on its services.**

Despite the geopolitical upheavals, Germany is on the verge of deepening its cooperation with Microsoft in 2025, even though the US company is pursuing a business policy that aims to make the state even more dependent on its services. Furthermore, the Redmond-based company wants to persuade its users to no longer purchase its standard software from Outlook to Teams and PowerPoint via perpetual individual licenses, but to only use it with a connection to Microsoft Azure cloud. Other connections to Office programs are to be phased out by 2029, such as on-premise software licenses.

Although there are individual alternatives to Windows, Office, Microsoft365 and Azure on the market and the first government players are already switching to alternative applications, Microsoft remains the top dog in public IT - both in the member states and in the EU.

A recent study by the Open Cloud Coalition has (once again) underlined Microsoft's dominant market share in the office software (*Office*, 90%) and collaboration (*collaboration*, 84%) sectors. A high market share of over 80% naturally also leads to high revenues for the quasi-monopolist: Microsoft recently received an estimated 198 million euros of German taxpayers' money for licenses for Office and operating systems. Microsoft in turn invests the profits in extensive lobbying activities that further programme the licensing regime and product logic for targeted and permanent dependencies.

There are various proposals for dealing with the German administration's dependence on Microsoft. A handful of these include a strategic exit from the Microsoft ecosystem by a set deadline, a binding requirement for open-source use in public IT procurement, to operating the Microsoft product range — including storing administrative data with a German company — and to strict, contractually guaranteed security measures and obligations by Microsoft itself.

In light of the current geopolitical situation, Germany and many other EU governments are striving for a state of "digital sovereignty". Much of this debate focuses on the promotion of digital infrastructure and industry in the EU. While these efforts are commendable at a political and abstract level, their concrete implementation requires time, clear strategies and extensive investment. Breaking free from the dependencies that have developed over decades would be a long-term feat. This white paper sets out which obstacles stand in the way of digital sovereignty and what would be possible - on a political level - within the current technological environment to give the administration more freedom of choice over its digital working environment.

In the following chapter this white paper explores how European public authorities and companies have become dependent on individual Microsoft products and show the disadvantages this entails for the state and the economy. Chapter 3 outlines the activities of the Microsoft group in the areas of lobbying and business model development, which are aimed at maintaining the existing monopoly position for operating systems and standard software in government digital workplaces. In Chapter 4, scenarios that can pave the way from the status quo to a "sovereign cloud infrastructure" in Germany and Europe are explored and in the final chapter a series of recommendations for action are formulated for political decision-makers.

Digital sovereignty
is not aimed at self-sufficiency or digital isolationism but is intended to give the state the opportunity to guarantee the technological freedom of choice to shape its digital working environment in accordance with strategy and the law. This goal cannot be achieved by striving for independence from non-European providers, i.e. only using European or German companies.

Rather, digital sovereignty means reducing practices that take away the state's freedom of choice over its digital infrastructure. Digital sovereignty means that the conditions are in place for a fair market environment in which customers have a real choice between software and cloud providers within and outside Europe. In the best-case scenario, the state would assemble its IT landscape in a modular and needs-oriented manner from interoperable components that communicate with each other via open interfaces. The opposite of digital sovereignty is de facto dependency on both quasi-monopolists and a "kill switch" abroad that can monitor, or completely paralyse, digital administrative work.

Chapter 2:

The status quo - The Microsoft empire and its background

The IT group, founded by Bill Gates in the USA in 1975, knows how to build, maintain and strengthen customer loyalty right from the birth of the cloud age. This is the result of years of intensive marketing and lobbying by

> **It is in the legitimate economic interest of an internationally successful IT group to consolidate and expand its market share in the public sector, so it is not surprising therefore that they may want to expand into other sectors.**

the Redmond-headquartered company. It is in the legitimate economic interest of an internationally successful IT group to consolidate and expand its market share in the public sector, so it is not surprising therefore that they may want to expand into other sectors. If the authorities are already relying on Microsoft for most of their computing systems, why not tap into other segments of government IT?

I. Microsoft‘s market power in the public sector and its causes

A recent study by the Open Cloud Coalition analysed Microsoft‘s dominant market share in standard software, in comparison to *Amazon Web Services* and *Google*. In the “Office” area, the authors calculated a market share of 90% and 84% in the “Collaboration” feature. This is why this white paper will focus on the “strongest player in the game” and not on its current competitors from the USA. Microsoft‘s market power is reflected in high utilisation and hence revenues from the public sector. In Germany, Microsoft incurs license costs of 197.7 million euros at federal level alone (i.e. not including figures from the 16 federal states and over 11,000 municipalities). Increased licensing costs has become an emerging trend: since 2017, costs at German federal level have risen by more than 250 percent, as reported by IT magazine heise. Of the total costs, 98.5 million is attributed to perpetual licenses, 29 million to subscription models and 69 million to “other services and products”.

A minor question in the German Bundestag at the beginning of 2025 revealed that the federal government relies on proprietary software for 99.9 percent of its operating expenses for cloud applications. Microsoft clearly has the highest share here. However, although there is much doubt and criticism in the digital policy discourse about the sensible and legally compliant use of Microsoft software with many questions still left unanswered (see X. below), numerous public bodies are still downloading Microsoft Teams. These bodies will then be tied into messaging, working on documents and holding video conferences on servers flanked by Microsoft licenses or subscriptions.

Does it make political sense for the anchor customer, the state, to be dependent on the strategic decisions of a single provider? In the following sections, we present some of the reasons why the German administration has become so dependent on a single provider.

1. Platform and lock-in effects favour dominant market position

Microsoft is so widespread on German public sector IT infrastructure that it cannot be explained solely by there being no alternatives to Microsoft on the market or that “MS” products are unbeatably good. It is more likely that Microsoft is using its political capital, which the company has built up and implemented for decades through lobbying activities and extensive public relations work, its market knowledge and its license management. This last being strategically rooted in its product development, from the Windows operating system and standard software (MS Office) to email servers (Exchange) and cloud (Azure / OneDrive), by

way of expanding its market share in the public sector. The company itself can hardly be blamed for its entrepreneurial success - it is trying to improve its sales and profits by whatever means possible; the responsibility lies with regulators, rather than expecting Microsoft to restrict itself.

In its market-penetrating role, Microsoft uses means that tend to undermine the goal of fair competition on the EU internal market. Its technical term is '*the lock-in effect*' where switching to another provider is deliberately more costly than sticking with the current provider, effectively keeping organisations from switching to a competitor. Thus, the principle of supply and demand fails. If those considering switching fear that a changeover will cost time and money, involve major internal changes and potentially lead to a loss of data, they will shy away from the change. Professor of competition law *Ruppert Podszun* describes lock-in effects as follows: "Due to thoroughly integrated, closed ecosystems, users are tempted not to leave these ecosystems in order to take advantage of alternative offerings, if interoperable at all". Through its strategy of product development in an exclusively Microsoft-dominated ecosystem, the company has managed to use lock-in effects to its advantage.

> **Microsoft also uses its dominant market position and financial leeway to shape the supply chain to suit its own objectives.**

Microsoft also uses its dominant market position and financial leeway to shape the supply chain to suit its own objectives. On several occasions, the Group has succeeded in forcing European competitors to play by its own rules, either through Microsoft sales techniques or turfing them out of the competition in other ways. The licensing system and sales channels have repeatedly come under criticism. In the area of cloud computing, Microsoft is said to have deliberately pushed independent cloud infrastructure providers into the role of resellers for Microsoft licenses.

2. Sovereignty exists only when there is freedom of choice – the perils of the MS-shaped devil you know

Windows and Office have claimed top spot for government computers and infrastructure, and now Microsoft also wants to expand its market share in the cloud. The company is exploiting several advantages in the cloud market, the first being power of habit. A quasi-monopolist benefits from a „We've always done it this way" mentality. Secondly, Microsoft can influence demand through its corporate policy regarding price and product development, and supply through its distribution network. As Microsoft is continuously increasing its global sales - it generated a net profit of €72 billion in 2024 -, the company also uses its financial leeway for extensive marketing and lobbying activities in Brussels and Berlin.

a) The power of habit in the public sector and the shortage of skilled workers

Strong forces of inertia are at work in the public administration. Anyone who wants to abandon the familiar Outlook environment or abolish Microsoft Word can expect much resistance at first. "We've always done that with Microsoft" can quickly become the rallying cry of an opposition trying to nip any notion of change within the digital working environment in the bud. Behind closed doors, political decision-makers cite such cultural challenges as the real reason for the reluctance behind building a pathway to a post-Microsoft era. Perhaps it is a convenient excuse. In any case, one thing is clear: if there is a lack of courage and drive for such a major project at a high political level, the inertia of the (official) masses usually wins out.

However, it is not only the users of standard software in the offices but also the administration's IT departments who may incur enormous additional costs when moving away from the familiar Microsoft ecosystem. The municipal IT officer quickly reaches his limits when even the data centre email accounts have been set up via Exchange, whose software is automatically updated with Microsoft tools such as Windows and Office Suite. After all, it is anything but child's play to replace an entire IT infrastructure that is heavily influenced by

Microsoft products and applications with alternatives. This is especially true when the unit also performs a variety of IT tasks itself, such as implementing OZG services, operating and maintaining the existing IT, processing IT support requests and receives little incentive and/or assistance for a changeover from the responsible departments. Moreover, the shortage of IT specialists does not stop at the federal state: working conditions can hardly keep up with the digital economy, and the management of public authorities often has little interest in digitalisation. And finally, schools and vocational colleges are so used to Microsoft that IT specialist training focuses on the Microsoft product range and its integration. Not only is there a lack of courage when it comes to change, but also a lack of personnel and skills resourcing in administrative IT to carry out this change.

b) When strategic product development and dynamic price development go hand in hand…

The announcement of a strategic decision at the headquarters in Redmond has put many customers in the public sector under pressure: with the switch to Microsoft 365, by 2029 Microsoft‘s top management wants it to no longer be possible to use on-premise variants of Microsoft programs (effectively phasing out Microsoft Office 2024 for example), making it imperative that all programmes have a connection to Azure cloud infrastructure. So, if the public sector wants to continue using the familiar Office environment, it will no longer have a choice from 2029, inevitably having to integrate even more deeply into the Microsoft ecosystem and adjust its budgeting to satisfy Microsoft’s cloud demands.

Pressure to move due to corporate decision instead of a cloud strategy reflective of the German administration’s needs

Despite the German administration not having been largely keen so far to switch to cloud computing, Microsoft’s recent announcement that only subscription-based models will be available from 2029 appears to be a strategic push toward a solution that may not fully align with the actual needs of public authorities. The signal from Redmond is clear: if authorities want to continue using Outlook and Office, it makes sense

> **The consequences of dependence on Microsoft are particularly clear at this point.**

to use the “public cloud” directly as a new storage medium and data hub for public administration. The consequences of dependence on Microsoft are particularly clear at this point. Instead of taking the first step in a cloud strategy to decide for itself and analyse when a cloud service can be sensibly used in the administration‘s workflow, the state is allowing itself to be driven forward by Microsoft‘s corporate decision to move towards cloud services, rather than searching for alternative providers that suit business needs. Actual freedom of choice over the state‘s own IT infrastructure would look very different.

The announced move away from the licensing model will foreseeably also have an impact on the central vehicle through which the German administration receives Microsoft licenses at special rates: Microsoft‘s framework agreement with the Federal Ministry of the Interior (BMI). This agreement forms the legal basis for the purchase of software licenses by German authorities and public bodies so that not only federal authorities, but federal states, municipalities and other bodies can benefit from discounted prices when procuring Microsoft licenses. They can make the so-called conditions contracts the subject of their procurement procedure. Cities and state authorities then purchase Microsoft licenses for standard software and server environments via the Microsoft Group‘s Licensing Solution Partners (LSP) - including Bechtle and SoftwareONE. Microsoft and the BMI negotiate new conditions every three years, usually for more Microsoft’s licensing products. The most recent three-year term did not begin until spring 2025. Microsoft‘s announcement to phase out the on-premise offer would not only affect the BMI framework agreement in terms of its structure and legal character. For the renegotiations up to 2028, it must be clarified how the so-called “Select Plus contract” must be adapted in view of future subscription models. The German government must now ask itself whether it should extend its existing contractual relationships with Microsoft considering the constantly growing ties and dependencies.

Prices, prices, prices - where is the journey taking us?

Microsoft has built a powerful lever through the pricing of its cloud, which enables the company to initially offer its existing customers very low prices to motivate the public sector to make a quick and painless decision to transition to their services. Gradually however, prices begin to increase over time. In the private sector market for cloud solutions, a price increase of 11% on April 1, 2023 led to massive criticism in Germany and Europe. Some competitors stated that the price increases "bordered on blackmail". The German Federal Cartel Office has also been closely monitoring the Group's pricing policy since September 2024, and has placed Microsoft under what is known as "extended abuse supervision" (Section 19a GWB). Microsoft had also claimed to private customers that its prices must also reflect fluctuations in the US dollar exchange rate and would therefore be regularly adjusted in future. A currency crisis in the USA or changes to import conditions could then lead to the German tax authorities being confronted with exponentially growing IT budgets - budgets that were perhaps reserved for expanding administrative digitisation and the promotion of sovereign cloud solutions.

Furthermore, if a private or public sector user of the Windows operating system or Office suite is supplied directly with a communication tool (Microsoft Teams) or a cloud application (OneDrive) - at first glance free of charge - this impairs free and fair competition, especially if other solutions are not interoperable with the Microsoft ecosystem at all. Instead of implementing a data protection-friendly messenger for public authority employees that is interoperable and thus guarantees the highest possible level of data portability in line with the GDPR, the public sector has been fed Microsoft Teams which intentionally fails to offer these functions - neither for free nor for a small surcharge. The EU competition authority takes a critical view of such business models. For various reasons, it can make sense for IT departments of public sector bodies to use Teams for internal communication given that servers and laptops are programmed for Microsoft anyway. Once Microsoft embeds itself into the core of the companies' IT operations, the next product update will lead to an automatic integration of new (MS) communication platforms too. This strategic approach has led to the German government finding itself in a gilded cage from which it can no longer easily escape. This development is currently being updated for the use of artificial intelligence, subsequently deriving from the cloud.

c) Enormous effort for lobbying and strategic communication

The high market share of Microsoft products in the public sector is no coincidence: it is in grand part due to intensive lobbying and public relations work by the Microsoft group. According to Lobbypedia, Microsoft operates "its own lobbying office in Brussels with 17 lobbyists (10 full-time equivalents)" and is the "largest lobbying force among tech companies in Europe". Lobbypedia estimates it spent "between €5,000,000 and €5,250,000" on lobbying activities in the 2019 financial year. According to statista, Microsoft invested seven million euros in political communication in the 2023 financial year – by contrast, Deutsche Telekom only spent €1.75 million and only Meta Platforms Ireland Limited spent €9 million. According to Lobbycontrol, Microsoft's PR work does not end with the company's own lobbyists. Microsoft is a member or sponsor of several think tanks, working groups and industry associations, from *Digital Europe* and the *European Internet Forum* to *the Centre on Regulation in Europe* (CERRE) to the *European Policy Centre* (EPC). There is also a network of agencies for political communication, advertising, political consulting and major international law firms.

In Germany, there are no exact figures on Microsoft's lobbying expenditure. The lobby register of the German Bundestag lists nine people for Microsoft Deutschland GmbH who "directly represent interests", and memberships in 50 associations are also recorded. Microsoft Deutschland GmbH is also a partner of the IT industry association BITKOM and a member of the Federal Association of the Digital Economy (BVDW), which regularly represent the interests of the digital economy in legislative procedures and public hearings.

In conjunction with the Group's overall strategy, comprising of 3,000 employees in Germany and 221,000 people worldwide, the Microsoft Group has an extensive network at its disposal to promote its own business interests in politics, public sector administration and society. The strong influence of big tech companies

during the legislative process for the new EU digital laws has led to critical reporting, with Microsoft often being the spearhead.

II Proprietary, insecure, illegal? - Criticism of the use of Microsoft in the German public sector

There are various facets to the criticism that the German public sector has become heavily dependent on Microsoft products. The central points are summarised below.

1. Lack of control over functionality and security of the software

Many government agencies rely on Microsoft for IT procurement primarily because it is easy and convenient to buy the accompanying bundles of Microsoft products on offer. Contrary to GovTech start-ups - a community of open source developers, companies and public IT service providers (from federal and state governments or European SMEs) -, politicians often lack the belief that they can develop Germany's IT infrastructure securely, functionally and reliably and operate it at a high level. Dependence on Microsoft is also convenient: to stop relying on Microsoft would mean the state potentially needing to provide IT infrastructure that had previously been outsourced to or purchased from Microsoft. Decision-makers fear that they will lack the financial leeway and human resources to switch to their own or more costly alternatives. And if a minister or state secretary fails with such a project, they not only jeopardise their own political reputation but also the ability of the government to function if the IT systems prove to be insecure or unreliable.

> **By purchasing licenses and subscriptions from a monopolistic player, governmental departments incur the side effect of losing control over the software and the inability to guarantee their own security, given they are left with little to no bargaining power.**

By purchasing licenses and subscriptions from a monopolistic player, governmental departments incur the side effect of losing control over the software and the inability to guarantee their own security, given they are left with little to no bargaining power. A key reason for this is that Microsoft treats code and system interfaces like trade secrets. Microsoft's business model consists of distributing 'proprietary software' via licenses. If the German government bases its digital workflows on Microsoft products, it only receives an installation file with a license key and, if required, support, but no insight into the source code. Microsoft's policy suggests a "take it or leave it" approach. Due to licensing restrictions, there is also no way for customers to adapt basic products to their own requirements. As the Microsoft ecosystem is deliberately closed, i.e. the standards and interfaces are not designed to integrate competitor products, the government can only build its IT landscape in a modular way to a limited extent. As the software is proprietary, so are the updates. Departments cannot check what is rolled out in detail to their computers and servers when Microsoft sends out a product or security update. The product adaptations take place globally, in private households and large companies, and are at best only peripherally oriented to the needs of German public sector organisations. When updates are rolled out, the state cannot reliably check on its own whether there are security vulnerabilities or backdoors in the code that make the IT infrastructure vulnerable. However, not updating software applications regularly for this reason would not be a good idea either: without updates, the products become increasingly insecure, partly because known security gaps ('n-days') remain vulnerable, leaving systems open to potential attackers.

> **As Germany has no influence on Microsoft's update policy and product development due to a lack of negotiating power of its own, its influence on its own digital working environment is considerably diminished.**

As Germany has no influence on Microsoft's update policy and product development due to a lack of negotiating power of its own, its influence on its own digital working environment is considerably diminished.

2. IT security and cyber security incidents

One consequence of the German state becoming so deeply involved in the Microsoft ecosystem is that it is beyond the independent control of the state whether public data on Microsoft servers is permanently secure

– either from access by foreign hackers or US intelligence services. If Microsoft not only offers individual software applications, but the German administration were to process large parts of its digital workflows via a complete Microsoft cloud environment, there would be more points of attack on the executive.

Trust in Microsoft can no longer be justified simply because it is the only guarantor of IT security in complex organisations. Several serious security incidents in recent years have demonstrated this, such as when one of the master keys for the encryption of the Azure cloud ended up in China. According to the BSI, this gave the hacker group Storm-0558 "access to email accounts of 22 organisations and government institutions, primarily in the USA, but not in Germany (...)." The danger here is that the key could also have been used to gain access to other Microsoft cloud services. The Cybersecurity and Infrastructure Security Agency (CISA) in the USA accused Microsoft of "multiple failures in cybersecurity" in an investigation report, as reported by heise.de.

The Microsoft Group has recognised it has issues with security. Its solution has been to forge strategic partnerships with international IT security companies or buy them up. IT security expert *Sandro Gaycken* described to rbb that the large digital corporations have "bought, consolidated and integrated cybersecurity companies into their products". The integration at Microsoft, for example, has given the company Crowdstrike "a market share of 14 percent", according to Gaycken. However, Microsoft's partnership with Crowdstrike backfired in 2024 when a security update from Crowdstrike for Microsoft applications contained faulty code. This resulted in systems failing and sensitive systems vulnerable to attackers. According to the company, 8.5 million Windows devices were affected worldwide, including operators of critical infrastructures in Germany, according to the BSI. The opposition in the Bundestag even described Microsoft as a "national security risk" following investigation.

In geopolitically turbulent times, with the world caught up in a hybrid war and escalating trade disputes, it is to be expected that attacks on sensitive infrastructures will increase rather than decrease in the future. Any cyberattack on and any vulnerability at Microsoft could then reflexively affect the German administration if it uses its digital infrastructure. Against this backdrop, IT security expert Sandro Gaycken sees only one solution: "We have to reduce our dependence on these very strong market leaders." At the same time, however, he adds as a warning that we are taking "a very big risk" and must be careful not to "do even worse" with "cheaper solutions".

3. Open data protection issues when using Microsoft 365

If the German state processes the personal data of citizens and its own employees, it is subject to the fundamental right of data protection. The EU General Data Protection Regulation aims to "ensure a high level of data protection" (Recital 6 Sentence 5 GDPR) and to safeguard the "fundamental rights and freedoms" of citizens and "in particular their right to the protection of personal data, whatever their nationality or place of residence" (Recital 2 Sentence 1 GDPR). If the administration uses software applications from a company to fulfil its national duties, these programs must also comply with data protection regulations. As Microsoft software is developed in the USA, and some was made available before GDPR came into force, complicated legal questions arise. Instead of setting up a new digital working environment for the German public sector in compliance with the "Privacy by Design" principle (Art. 25 GDPR), data protection analyses has revolved around trying to make Microsoft product functions fit into data protection regulations, with limited success. Ultimately, this was a result of the German state's own lack of negotiating parity: where a provider has a monopoly over software and cloud products, it becomes increasingly difficult to enforce adherence to data protection conditions.

This dilemma has amounted to various legal uncertainties: the question of whether the use of the cloud-based Microsoft365 application in the public sector is compatible with the GDPR has always divided opinion. Numerous data protection experts - including the Data Protection Conference (DSK) of the German supervisory authorities - are of the opinion that Microsoft365 applications cannot generally be used in compliance with data protection regulations. In November 2022, the DSK came to the following conclusion: "As long as the necessary transparency regarding the processing

of personal data from order processing for Microsoft's own purposes is not established and its legality is not proven, this proof cannot be provided." In addition to the lack of transparency regarding the functions and data flows of the application, the criticism also focuses on untraceable data transfers and the extensive collection of diagnostic data by Microsoft "in the background".

In July 2025, the European Data Protection Supervisor came to a different conclusion following a lengthy investigation into the use of Microsoft365 by the EU Commission. In his view, there were no longer any objections to the use of Microsoft365 after numerous technical and legal adjustments. The European Data Protection Supervisor argues that "additional contractual, technical and organisational measures that have been implemented or are planned in cooperation with Microsoft" have dispelled the data protection concerns. This is based on the conviction that, through detailed analysis of the Microsoft365 software environment, it is possible to formulate the conditions for product adjustments that would bring Microsoft365 into compliance with the GDPR. However, the exact documents and assurances provided by Microsoft as part of the proceedings are not available to the public. It also remains unclear whether other supervisory authorities or even courts agree with the assessment. As a result, the European Data Protection Supervisor's decision does not improve data protection through the fair negotiation of the framework conditions for cloud use, instead it merely tinkers with the problems without addressing the actual cause - the cause being the result of decades of dependency on a single provider.

Chapter 3:

IT can't live with, or without, Microsoft? Is a "sovereign" cloud possible?

There is currently no such thing as a digitalised public administration without Microsoft. Neither in Germany nor internationally. No other company has been able to catch up with Bill Gates' tech empire in home and work computing - even in the cloud age, this does not look likely to change anytime soon. Only China it seems, with *Alibaba Cloud* and *Tencent Cloud*, can fall back on domestic solutions in the cloud market.

But is the German administration's dependence on Windows, Office and Teams set in stone?

One thing is clear: in an ideal world, the German state would not be reliant on individual providers and would be able to put together the right offering from a wide range of IT providers' portfolios. A laptop from one, an operating system from another, an office environment from the other and a mail server from somewhere else - where everything can be connected and exchanged on a modular basis. Open interfaces would be standard. The state could commission secure and easy-to-use solutions and have them tailored to meet the regulatory and user-oriented needs of the administration. There would be multi-cloud infrastructures and clear open source obligations in the award conditions. There would be no doubt that government data cannot be transferred to third countries or that the software environment can be controlled or even shut down remotely from another continent.

But the reality is that German authorities have become deeply embedded in the Microsoft ecosystem and continue to depend on the company's software for their day-to-day work. A sudden transition and changeover is therefore not very realistic. Even if individual federal states were to attempt it alone, this can become a one-way street if no one joins in the long term. This is because all players would have to initiate such a shakeup together to redefine the best conditions, demand these contractually and push for acceptable prices as well as establish common interfaces for exchange within the federal state. So why is this not happening?

In the 1990s, there were two titans of digital office equipment: Microsoft and Apple. They built two competing empires of operating systems, which - to this day - are hardly interoperable with each other. As the German administration is subject to the principle of economic efficiency, the cheaper PC workstation with Microsoft Windows and Microsoft Office became the standard in the offices. This marked the beginning of the era of software licenses, which took the following form: Microsoft issued licenses to its products (by itself or through third-party companies), thereby establishing commercial relationships and supply chains with almost all German authorities that wanted to equip themselves digitally. This distribution network, aka the Microsoft ecosystem, quickly began dominating decisions in municipal and state procurement departments, and still does so to this day. The associated field of IT procurement has only developed legally, organisationally and strategically over the years in parallel with the digital transformation.

As the German administration is subject to the principle of economic efficiency, the cheaper PC workstation with Microsoft Windows and Microsoft Office became the standard in the offices. This marked the beginning of the era of software licenses

There have repeatedly been political strategies - including large-scale ones - to break free from existing

dependencies and take a confident step into the cloud age. The field of cloud computing is teeming with ideas and strategic approaches, such as the:

- IT consolidation Bund
- Multi-cloud strategies such as the "German administration cloud"
- The "Sovereign Cloud Stack"
- Cloud computing initiatives at EU level
- The "Open Source Week" at UN level in 2025

However, it is a long way from the strategy papers, pin boards, mind maps and presentation slides required to challenge Microsoft's digital standing with the German public sector. Without a clear steer from political leaders, even with internal and external support of resistance to MS products, as well as in-depth knowledge of the existing ecosystem and alternatives, such a large-scale IT project cannot succeed.

The governmental structures in Germany make it even more difficult to reach a political consensus on breaking new ground, launching an open and modular IT system and leaving existing dependencies behind. This is because the federal states and local authorities are free to decide how they equip their authorities in terms of personnel and technology: some authorities already work with Microsoft365 and communicate internally via MS Teams; others use open video conferencing solutions and messengers, but operate their mail servers with MS Exchange; others are still on the status of on-premise licenses for Outlook, Word, PowerPoint without a cloud connection. Meanwhile, Microsoft, SAP and others offer Delos Cloud, which allows Microsoft365 to be operated in a cloud that is not hosted on Microsoft servers, but at a subsidiary of SAP (see below).

So, when the 'trusted' Microsoft sales partner in the IT department comes by and touts the new services available, many a head of department is tempted to buy these "innovations" from Microsoft. The coronavirus pandemic has exacerbated this trend. With the contact bans and government closures, it was clear that the administration had to remain operational - to do so, it had to communicate digitally, share data and remain connected to the existing infrastructure at the same time. In the view of many decision-makers, relying on Microsoft was the safest and quickest way to achieve this. Once again, such IT operations were already in place that the general view was that Microsoft365 or Teams were "already here" and can no longer be easily reversed.

As a result, the freedom of choice for European users has been significantly diminished by targeted licensing and bundling tactics, constant lobbying and business models that have achieved market dominance through lock-in and platform effects. Although alternative IT groups are already working together within the framework of procurement procedures to break up this monopolisation in the cloud sector, there is currently no sign of companies being prepared to pull together of their own initiative. In June 2025, Reuters reported that Telekom, IONOS and Schwarz did not want to throw their hats into the ring as a joint consortium for new EU programs. However, a cleverly designed and federally coordinated process to develop and operate an open alternative to Microsoft Office and the Microsoft cloud environment in a consortium could create the digital work platform of the public administration of the future in an open, free and functioning digital ecosystem.

Chapter 4:

Product adaptations and offerings from Microsoft between serious effort and sovereignty-washing

In order to respond to the criticism of its business model under data protection, digital policy and competition law and to convince political decision-makers that Microsoft products remain the best choice for the German administration, the company has made or proposed various adjustments to its products.

I. European security program

In June 2025, Microsoft announced a "European Security Program". As part of the program, Microsoft intends to share AI-based threat intelligence with governments and provide real-time security-related data following ongoing cyberattacks on the Microsoft ecosystem. The Group intends to use the program to invest in local cyber security capacities and the digital resilience of states, authorities and civil society. New partnerships with law enforcement agencies and organisations such as Europol are meant to combat cybercriminals and state-sponsored attacks more effectively. Microsoft wants to detect malicious infrastructures and counter-attack crises more quickly and deactivate them automatically.

In view of the hybrid threat situation in cyberspace, which BSI, intelligence services and security politicians have been pointing out for years, it makes perfect sense for Microsoft to use its capacities as a global corporation to support the security of government IT systems. In particular, Microsoft wants to offer free assistance against new forms of cyber-attacks that are orchestrated and carried out using AI. Given the incriminating headlines relating to Crowdstrike and the Masterkey for Azure cloud in past years, it is unsurprising that the European Security Program also resembles a marketing campaign ploy. Now, in uncertain times, Microsoft is suddenly offering its support as an IT grand master to protect the European continent from stormy times in the digital space.

II. Individually negotiated data protection conditions

The data protection authorities at national and EU level have always criticised the use of Microsoft products, especially with regard to the cloud-based Microsoft365 for not being sufficiently transparent and having control over the data flows in Microsoft's machine room (see above). As an international company, Microsoft also had to deal with the challenge of formulating data protection conditions that were tailored to each region of the world and every regulatory environment – as well as adapting the product range technically.

When organisations purchase standard software, they often lack the opportunity to negotiate terms individually when dealing with large international corporations. Instead, they have to make do with the general data protection terms in their market or sector. Following criticism from the State Commissioner for Data Protection and Freedom of Information (LfDI) and the DSK, some state governments have now broken this dependency on standard clauses in data protection conditions, as reported by the computer magazine c't 2024.

The state of Lower Saxony has negotiated special rules with Microsoft. Microsoft has promised that data storage and processing will only be carried out on European servers, while IT support will come from countries that allow it to work with Microsoft in a "GDPR-compliant" manner. Data outflows from the EU servers and data transfer to the USA for "background analyses" or support would then still be possible in accordance with the contract but would tend to be reduced in scope. Part of the individual conditions could also be that only certain categories of data are processed and transferred for support purposes, as the EU Commission has seemingly negotiated with Mic-

rosoft. Even so, it would remain questionable whether the assurance and actual practice are really compatible. The “Cloud Act” problem would also remain unresolved.

In addition, Microsoft is shutting down individual services in Lower Saxony that are particularly opaque about background operations - e.g. diagnostic data and Teams Analytics. Here too, however, it remains to be seen whether this alone will effectively prevent large data outflows or whether they can be sufficiently controlled, and how the administration would react if Microsoft were to drastically increase its prices later on or deactivate and restrict licenses or subscription models.

In addition, the authorities want to ensure that certain particularly sensitive data - e.g. social or health data - is not processed and exchanged via MS Teams by means of internal work instructions for handling Microsoft products. As the human factor is often the biggest weak point, and internal guidelines are difficult to enforce or monitor across the board, there is still a considerable degree of residual uncertainty.

III. The Delos solution: Data centres operated by European companies - (only) software comes from Microsoft

But what if cloud-based Microsoft products à la Microsoft365 were provided on shielded data centres of European companies to which only public authorities are connected? This would theoretically ensure that any backflow of data to the USA is restricted to remaining “in the background”. Even if the US government were to ask the company to provide European data, Microsoft would not actually be able to do so. This is because control would lie solely with the operators of the data centres.

A consortium consisting of Microsoft, SAP and Arvato has set out to solve the dilemma of international data transfers. A public authority could then book cloud services from Microsoft via Delos GmbH, a subsidiary under the control of German internet giant SAP, and would avoid having to purchase software and infrastructure directly from the Microsoft Group and have it operated on its infrastructure. There is a similar solution in France: Capgemini and Orange have founded the joint venture “Bleu” there. The promise of Bleu and Delos is to erect data centres and data under national control, with only software updates coming from Microsoft in the USA. At first glance, it sounds tempting when the SAP subsidiary Delos promises:

> “The services of the sovereign cloud platform include, in particular, the extensive collaboration tools and productivity solutions of Microsoft Office 365. The cloud platform will be technically, operationally and legally sovereign in accordance with federal regulatory requirements. Delos Cloud is currently the only cloud offering to fully comply with the requirements of the BSI for IT security and confidentiality as well as the legal requirements for data protection in coordination with the Federal Commissioner for Data Protection and Freedom of Information (BfDI). As the owner of the infrastructure, Delos Cloud GmbH is responsible for both the platform operation and the licensing of its products.”

One disadvantage of the corporate construct is that prices are 15 percent more expensive than the “Microsoft pure” variant with the standard Microsoft Cloud, as reported by Computerwoche. The higher price is economically understandable, as the Delos clouds involve far more effort than simply purchasing a license from the standard Microsoft product range. From the perspective of the individual state or local authority, there would then be a choice between “pure Microsoft” via the BMI framework agreement and the more expensive “Delos” variant.

However, whether the solution really provides effective protection against data leaks to US security services, hacker attacks due to a lack of IT security or tougher measures in trade disputes with the Trump administration is another matter. Delos CEO Georges Welz reported in an interview with heise: “As the cloud is under our control, no one can immediately restrict operations. And if there are no more updates, we could continue working for months because the cloud also works independently. In this respect, we definitely offer sovereignty, namely a period of time to react.” This al-

ready indicates that, in the worst-case scenario, long-term operation of the Delos Cloud would no longer be possible. This would jeopardise the functioning of the entire administration. The transition period, which Welz describes as "over months", could be reduced to 0 days if, say, it became known that the last update of the systems - as in the Crowdstrike case (see above) - had led to an open security gap.

And completely independent of the aforementioned technical arguments, the following also applies here: a semi-sovereign solution such as Delos would in no way make Germany more independent in its procurement decisions, as the state, as the primary customer, would continue to be bound to the group's software and its restrictive license conditions. Despite the legal construct of using an intermediary from Germany in the form of Delos, all technical paths would ultimately lead back to Microsoft. As a result, the solution may give the impression of digital sovereignty, but in reality the old dependencies would continue to exist under a new guise.

IV. Data boundary and local instances

In response to fears that the US government could access public administration data and communication content, Microsoft has announced three further measures: a data border, data guardians and locally operated instances.

On the one hand, Microsoft wants to introduce a "data border" into its complex processing procedures for the "Sovereign Public Cloud" offering. In terms of content, this is in line with the data protection conditions individually negotiated by Lower Saxony in that all customer data will only be processed within EU borders. In addition, there is a slight alteration when it comes to encryption which is important for data security, and this is that the master key ("encryption key") is to remain exclusively with the client.

With the "Data Guardian" measure, Microsoft promises that admin access to European cloud services will only be exercised by Microsoft employees residing within Europe. Should remote access from the USA be necessary in certain cases for complicated support issues, this will only be possible with the express permission of European colleagues. In this way, it should be less common for people outside the EU to gain access to the cloud infrastructure.

> **According to Microsoft, "Microsoft 365 Local" will also allow the software environment to run without a fixed and permanent connection to the Microsoft cloud environment in the future.**

According to Microsoft, "Microsoft 365 Local" will also allow the software environment to run without a fixed and permanent connection to the Microsoft cloud environment in the future. This would allow it to continue to run on its own infrastructure if the authorities see no reason to use a cloud-based solution. Is this ultimately a departure from the announcement that on-premise software will no longer be offered and further developed from 2029 - or an integration of a somehow more secure Microsoft365 local variant "for subscription or cloud products", which *Andreas Thys* describes as "bizarre" in his guest article?

Even if data processing were to take place exclusively within the EU under the responsibility of EU subsidiaries that are fully subject to the GDPR, the question remains as to how "sovereign" such measures will really make public administration in the medium to long term. In Andreas Thyen's view, the "countermeasures now presented - EU Data Boundary, Data Guardian, locally operated instances - (...) are targeted PR measures. The hope is for maximum control without having to relinquish technical sovereignty." The Research Director of the cyberintelligence.institute, Prof. Dr. Dennis-Kenji Kipker, comes to the conclusion: "The security promises are built on sand". This is because, according to Kipker in a commentary on IT Daily, upon closer inspection it is neither a real data boundary nor true sovereignty over a user's data, which is stored in Microsoft's cloud. Prof. Dr. Harald Wehnes, spokesperson for the "Digital Sovereignty" working group of the German Informatics Society, puts it even more dramatically: "Under the guise of 'digital sovereignty', tech companies are clearly pursuing the goal of luring Europe into irreversible and expensive bogus solutions. These

are intended to consolidate their market power and ultimately even give them more control over data and technologies.” These statements make it clear that it does not matter which path Microsoft takes - in the end, the proposed “alternative measures” also deepen dependency and bind customers even more strongly to a closed environment, which is the opposite of digital sovereignty. The underlying dominance of Microsoft, with its ability to dictate terms and bind customers to it through licenses and other means is not changed in any way by the proposals.

These statements make it clear that it does not matter which path Microsoft takes - in the end, the proposed “alternative measures” also deepen dependency and bind customers even more strongly to a closed environment, which is the opposite of digital sovereignty.

Chapter 5:
Summary and recommendations for action

Microsoft products dominate the working environment of public administration. Even in the future market of cloud computing, the top dog wants to retain and expand its market share in the public sector. After all, the more networked the administration becomes, the more important it will be not only to process and store documents locally in official silos, but also to use IT systems collaboratively and digitally across government boundaries. With its announcement that it will switch to subscription models with mandatory Azure subscriptions from 2029, Microsoft has put the German administration under pressure to act. At the same time, this opens up a window of opportunity to strategically plan and gradually implement a switch to an open, secure and sovereign digital working environment for the public sector. In this way, the political priorities of digital sovereignty, data protection and cybersecurity could be realised through tailor-made solutions instead of remaining in a closed ecosystem with strategic disadvantages.

With its announcement that it will switch to subscription models with mandatory Azure subscriptions from 2029, Microsoft has put the German administration under pressure to act.

As Microsoft wants to further expand its market share in the public sector and consolidate its position in cloud computing, the company is using all its marketing power to respond to the complex criticism and publicly debated security incidents. On the path towards a "sovereign cloud" in Germany and Europe, a cat-and-mouse game can be observed between digital policy and data protection criticism and ever new announcements from the Group. Even if each of the measures attempts to address individual points of criticism and mitigate certain risks, the existing dependencies of the German administration on the Microsoft product range and the risk of a loss of control or significant data leaks remain.

As a result, the close cooperation between the public administration and Microsoft repeatedly leads to criticism in several central aspects: data protection and transparency, data, cyber security and monopolistic cloud coercion instead of an independent cloud strategy. The extensive proposals and product adaptations that Microsoft has presented in recent years only partially or rudimentarily address these four central concerns. This is due to the enormous market dominance of an international corporation and its business model, which has been questionable for decades in terms of competition, a closed ecosystem and dynamic business concept development and pricing policy. All these indicators stand in the way of achieving a digitally sovereign working environment for public administration in Germany. It is time for a strategic realignment. If "digital sovereignty" is understood as freedom of choice and the ability to control the state IT infrastructure and official data flows, only a complete realignment of the public IT landscape can lead to this goal in the long term.

The central legal and political vehicle for controlling the specific integration and contractual cooperation with Microsoft is the BMI framework agreement with the company. The terms of the framework agreement concluded in spring 2025 cannot be changed **in the short term** in the next three years, but the time can be used to be prepared **in the medium term** for a possible extension in 2028 and to initiate a complete realignment towards "digital sovereignty" with open software and a sovereign multi-cloud strategy **in the long term**.

Short-term measures until 2028:

- **Monitoring of IT procurement costs via the BMI framework agreement by the federal government**
  The federal government and the Digital Ministers' Conference (DMK) should provide themselves and the public with a precise overview of how much taxpayers' money the federal, state and local governments are currently spending on Microsoft licenses. In addition to a systematic survey of the respective items at federal, state and local authorities, the financial authorities could also ask the Licensing Solution Partners (LSP) to disclose how much revenue they generate annually with the business model "license purchase based on the BMI framework agreement". Without reliable figures, the financial scope for a change in strategy cannot be calculated and planned.
- **Feasibility and potential studies for increasing freedom of choice in individual product areas**
  Based on the monitoring of overall costs, the German government and DMK should examine several scenarios in the direction of freedom of choice and digital sovereignty as well as their political, legal and technical framework conditions in feasibility studies for an open, interoperable and fair cloud market. Particular attention should be paid to the product areas of operating systems, office software, communication (email and messenger), collaboration (collaborative work on documents and shared data storage) and multi-cloud services to overcome the existing dependency on a single provider. The economic and technical analysis should forecast whether alternative offerings could be strategically procured and implemented in the future based on annual expenditure and current IT equipment. If gaps in the market are identified, the study should also look at how the federal and state governments could specifically close these gaps through research and company funding. The potential analysis should also include interviews with companies in the Microsoft ecosystem, European competitors, contracting authorities in state and local government with consumer protection and business associations in order to take a closer look at figures and business strategy.
- **Intensify competition law investigations into the Microsoft ecosystem and licensing with a view to public administration**
  As part of its investigations under Section 19a ARC, the Federal Cartel Office should set up an independent working group to take a detailed look at the Microsoft Group's distribution network and the use of Microsoft products in public administration. The budget legislator should provide the authority with sufficient resources to investigate and, if necessary, break up anti-competitive monopolies. A broad-based investigation alongside the EU Commission and other member states can reveal the extent to which the market-dominant position is maintained or deepened by contractual conditions for license, cloud and framework agreements. It is important to also consider the influence and control options of the Microsoft Group and its often exclusive sales partners in public procurement or in complex procurement processes. All business practices that stand in the way of fair competition and genuine freedom of choice - in particular restrictive licensing practices - should be identified and prevented with appropriate regulatory measures.
- **Strategic digital dialogues with international partners on the issue of digitally sovereign administrative IT**
  The Federal Government should establish and promote strategic international dialog formats in which the Federal Republic of Germany engages in a structured exchange with the EU Commission and other EU member states (e.g. Italy, France, the Netherlands, Portugal and Estonia), but also with strategic partners worldwide (e.g. South Korea, Japan, Canada or Australia) on the path to sovereign public sector computing. In doing so, it should involve civil society, science, but also European companies and the open source community. The scope and range of the strategic digital dialogues can be conceived and designed in vastly different ways. In addition to an institutionalised exchange of experience at various levels, through the collection of best practices in the area of IT sovereignty strategies, joint research projects or even transnational development contracts for individual IT solutions, the formation of a joint negotiating group for strong and uniform framework agree-

ments with Microsoft. Where the Microsoft Group has been able to gain a negotiating advantage in framework and license agreements with its close-knit sales networks and highly qualified law firms, public clients should also gain negotiating advantages through the exchange of experience and knowledge transfer.

Medium-term measures for the negotiations on the next BMI framework agreement:

- **Freedom of choice "light": choice between new and old Microsoft products**
  It makes economic sense that Microsoft now wants to switch from its model of perpetual license purchases to a subscription model. This will give the company more leeway under contract law and enable it to prevent abusive license use more effectively. From a public administration perspective, however, switching to cloud-based solutions would be the third step before the second. The administration already has software licenses, particularly for standard office software, and in many areas there is no urgent practical need to abandon the on-premise use of Outlook, Office or Messenger. Nevertheless, the state should negotiate confidently and also consider the option of a strategic switch to alternatives. With the announced discontinuation of on-premise solutions from 2029 and the associated necessity of a forced switch to the Microsoft cloud, this problem is already acute. Therefore, it is imperative to create the legal and factual framework conditions for real freedom of choice on the cloud market as quickly as possible.
- **Contractually enshrine cost transparency regarding license costs at all levels**
  The fact that Microsoft has precise figures on its business volume with the German administration, but the public regularly has to estimate how much tax money flows into Microsoft licenses, is an untenable situation. In the negotiations on a framework agreement, the German government should insist on a monitoring instrument that makes it possible to document the annual expenditure on Microsoft licenses or subscriptions in a low-threshold and publicly comprehensible manner. Based on this data, the federal and state governments could forecast much more accurately which price advantages and volumes they need in the respective budget years. Synergy effects could be achieved and existing information asymmetries vis-à-vis Microsoft could be reduced through cooperation between IT procurers at federal, state and local level. It is in line with the principle of economic efficiency and thriftiness of the administration to handle taxpayers' money prudently and sustainably.
- **Adapting licensing modalities to the needs of the administration**
  In preparation for the negotiations on a new framework agreement with Microsoft, the federal government, the federal states and the municipal umbrella organisations - for example within the framework of the DMK or in the IT Planning Council - should prepare very thoroughly together and, if necessary, seek outside help. At the very least, this includes precisely forecasting the respective requirements and budgets and obtaining certainty about the extent of the desire for on-premise, Microsoft365 or public cloud. In addition, the state could consider making changes to the existing sales network via licensing solution partners and taking on a more controlling role in licensing itself.
- **Mandatory audits and transparent real-time analysis of data flows**
  The German government should oblige Microsoft to allow extensive audits with insight into the program code before new software applications or extensive updates are used in public administration. Only through a real insight can it be verified whether data protection on paper actually corresponds to the technical processes in the machine room. The state can assure the company of confidentiality. The German government should also work to ensure that all remote access to the Microsoft infrastructure is logged in an unalterable manner. The state should have a precise overview of who accessed the system when and for what reason - and what data was transmitted to the USA for this purpose.
- **Interoperability and open interfaces as a contractual obligation**
  Based on feasibility studies and investigations by the Federal Cartel Office, the German government should explore where it can oblige Microsoft to provide interoperability with other products and open interfaces in a framework agreement. As long as the Microsoft ecosystem is deliberately closed and can

exploit lock-in effects, dependency will be reinforced rather than reduced.

With all of this in mind, the German government may well threaten to withdraw from the framework agreements by a certain deadline if the Microsoft Group's skilled negotiators reject certain demands.

Long-term measures for the era of digital sovereignty in the EU and Germany:

The 1990s, when the choice rested between Apple and Microsoft, are long gone: the IT market has become highly differentiated, even if this is not reflected in Microsoft's market share in the public sector due to its dominant market position. In the long term, Germany would be well advised to establish a functioning and interoperable system with various providers and products; a kind of IT department store where the individual authorities can help themselves and put together the solution that suits them best. With the "EuroStack" and "Deutschland Stack" initiatives - admittedly not yet clearly defined in terms of content - Brussels and Berlin are already programmatically setting out on the path to digital sovereignty. Words must soon be followed by deeds. It is important to learn from political failures such as the "gaia x" initiative and not repeat mistakes.

> **In the long term, the federal and state governments should ask themselves: wouldn't it be better to invest taxpayers' money, which is spent every year on licensing costs for Microsoft products, in a diverse network of IT providers that reduces excessive dependence on a single monopolist and enables digitally sovereign solutions?**

In the long term, the federal and state governments should ask themselves: wouldn't it be better to invest taxpayers' money, which is spent every year on licensing costs for Microsoft products, in a diverse network of IT providers that reduces excessive dependence on a single monopolist and enables digitally sovereign solutions? This could create a software environment and thus a digital working basis for the administration that is easier for the state to control and manage. Specialist authorities such as the BfDI, Bundeskartellamt and BSI could define the requirements for data protection, IT security and fair competition - and oversee the actual implementation. As a result, the administration would have freedom of choice and could plan costs in the short, medium and long term. To ensure cyber security, the state would no longer have to rely on a fragile trust that Microsoft will protect its systems from attacks.

In the best-case scenario, an openly competitive digital working environment would be created for public administration that other countries would also want to use: a German stack with an international community, constantly growing services and the maxims of interoperability and modularity as the core of the brand. On the basis of the short-term and medium-term measures, in particular a valid numerical basis on tax funds used and feasibility studies, the German government could identify a date from which the exit from the Microsoft ecosystem towards a sovereign working environment for the administration should take place. All stakeholders could then gear their strategic planning towards this exit date. However, they will only do this if there is a clear "announcement from above" - ideally from the Federal Chancellery and the state chancelleries.

> **It is a good sign that the new Federal Ministry for Digitalisation and State Modernisation (BMDS) is planning an entire department for the "Germany Stack".**

It is a good sign that the new Federal Ministry for Digitalisation and State Modernisation (BMDS) is planning an entire department for the "Germany Stack". It would be an internationally respectable success for the new Federal Minister Dr. Karsten Wildberger if he manages to lead Germany from digital dependency to digital sovereignty. If he successfully launches the mammoth project of freeing Germany from its strategic dependence on Microsoft products during his first term of office, and is also prepared to stand up to the hitherto near untouchable tech giant Microsoft, insofar as it is in the interests of the German state, he would have done credit to his reputation as a crisis manager for major IT projects. It would not only be a political success, but in the best-case scenario also an economic stimulus program for the domestic digital economy and a valuable increase in digital freedom of choice and decision-making for everyone.

CYBERINTELLIGENCE
.Institute

Imprint

The author
Michael Kolain is a fully qualified lawyer and digital policy expert. He works at the interface between legislation, science and the development of digital technologies.

---

cyberintelligence.institute (Publisher)
MesseTurm
Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.

T +69 5050 34-602

www.cyberintelligence.institute
info@cyberintelligence.institute
