



Bericht 2026-DFIN-22

22. September 2026

Schluss mit der Abhängigkeit von Microsoft! (Für die digitale Souveränität des Kantons Freiburg)

Wir unterbreiten Ihnen hiermit den Bericht, der dem am 16. März 2026 an den Staatsrat überwiesenen Postulat 2026-GC-64 Kirthana Wickramasingam / Pierre Vial direkt Folge leistet.

Inhalt

1	Zusammenfassung des Postulats	2
2	Bericht des Staatsrats	2
2.1	Allgemeines	2
2.2	Rechtliche, finanzielle und organisatorische Fragen zu Microsoft Office 365	2
2.3	Alternativen und digitale Souveränität	4
2.4	Aktionsplan und innovativer Ansatz	5
2.5	Fazit	6

1 Zusammenfassung des Postulats

Mit einem am 16. März 2026 eingereichten und begründeten Postulat stellen Grossrätin Kirthana Wickramasingam und Grossrat Pierre Vial fest, dass sich der Staat Freiburg für einen weitgehenden Einsatz der Bürosoftware-Suite Microsoft Office 365 entschieden hat. Sie sind der Ansicht, dass die flächendeckende Nutzung dieser von einem ausländischen Unternehmen entwickelten und betriebenen Office-Suite in Bezug auf Datenschutz, digitale Souveränität, technologische Abhängigkeit und Marktzugang in mehrfacher Hinsicht äusserst problematisch ist.

Das Postulat fordert den Staatsrat auf:

1. die rechtlichen, finanziellen und organisatorischen Auswirkungen der derzeitigen Nutzung von Office 365 in den Schulen, der Kantonsverwaltung und im Parlament zu prüfen, insbesondere im Hinblick auf den Datenschutz und die digitale Souveränität;
2. alternative Lösungen zu evaluieren, insbesondere solche, die Garantien für Datenschutz und Souveränität bieten und lokal oder in der Schweiz gehostet werden;
3. einen mittelfristigen Aktionsplan zur Umsetzung dieser Lösungen in Schulen, Verwaltungsstellen und politischen Gremien vorzuschlagen.

2 Bericht des Staatsrats

2.1 Allgemeines

Der Staatsrat teilt die Bedenken der Verfasserin und des Verfassers des Postulats hinsichtlich der digitalen Souveränität, des Datenschutzes und der technologischen Abhängigkeit. Die weit verbreitete Nutzung digitaler Lösungen grosser internationaler Anbieter, insbesondere von Microsoft, wirft berechtigte Fragen auf, die der Staatsrat in seiner Strategie zur Governance der Informationssysteme berücksichtigt.

Die in diesem Postulat aufgeworfenen Fragen sind im Rahmen der Governance der Digitalisierung und der Informationssysteme des Staates zu betrachten. Gemäss der Verordnung über die Governance der Digitalisierung und der Informationssysteme des Staates (SGF 122.96.11 GDISV) legt der Staatsrat die strategische Ausrichtung der Digitalisierung über den Richtplan der Digitalisierung und der Informationssysteme fest. Der Richtplan soll insbesondere die Informationssicherheit, die Aufrechterhaltung öffentlicher Dienstleistungen, die Kontrolle über digitale Risiken, die Interoperabilität der Systeme und den effizienten Einsatz von Ressourcen gewährleisten. Das Amt für Informatik und Telekommunikation (ITA) spielt eine zentrale Rolle bei der Umsetzung dieses Vorhabens, denn es kümmert sich um die technische Seite der digitalen Infrastruktur und E-Services des Staates und begleitet die Projekte zur digitalen Transformation der jeweiligen Direktionen und Anstalten.

Für den Einsatz von Microsoft 365 sind jedoch mehrere Faktoren ausschlaggebend: die funktionale Vielfalt, das hohe Mass an Integration und Sicherheit, die technologische Reife sowie die sehr grosse Verbreitung sowohl in öffentlichen Verwaltungen als auch in privaten Unternehmen und Bildungseinrichtungen. Das alles trägt zur Gewährleistung der Betriebsabläufe, der Interoperabilität und der Produktivität der Mitarbeitenden des Staates bei.

2.2 Rechtliche, finanzielle und organisatorische Fragen zu Microsoft Office 365

Der Staatsrat hält fest, dass sich die Abhängigkeit des Staates Freiburg von Microsoft nicht allein auf die Microsoft 365-Suite beschränkt. Sie betrifft ein viel breiteres Spektrum an IT-Komponenten, darunter insbesondere Betriebssysteme, Identitätsmanagement-Tools, Serverinfrastrukturen und verschiedene Fachanwendungen.

Diese Situation ist das Ergebnis einer schrittweisen Entwicklung über mehrere Jahrzehnte hinweg, in einem Kontext, in dem sich Microsoft-Lösungen in der westlichen Welt de facto als Standard etabliert haben. Daher müssen alle Überlegungen zu einem Ausstieg aus dieser Abhängigkeit ganzheitlich, strategisch und langfristig angegangen werden.

Der Staatsrat ist sich der Herausforderungen im Bereich des Datenschutzes bewusst, insbesondere was das Hosting und die Verarbeitung sensibler Informationen betrifft. Es werden vertragliche, organisatorische und technische Massnahmen umgesetzt, um ein Schutzniveau zu gewährleisten, das den Anforderungen des Bundes- und Kantonsrechts entspricht. Zu diesen Massnahmen gehören insbesondere die vertragliche Regelung der an externe Dienstleister übertragenen Datenbearbeitungsaufträge, die Erstellung von ISDS-Konzepten¹ und Datenschutz-Folgenabschätzungen (DSFA²) sofern erforderlich, die Implementierung starker Authentifizierungsmechanismen, die Verschlüsselung der Kommunikation sowie regelmässige Sicherheitskontrollen.

Der Staatsrat räumt jedoch ein, dass der internationale rechtliche Kontext, insbesondere in Zusammenhang mit bestimmten ausländischen Rechtsvorschriften, zu Rechtsunsicherheit führen kann. Diese wird aufmerksam verfolgt. Nach einer Reihe von Analysen und Berichten hat der Staatsrat mehrfach die Vorteile, Risiken und organisatorischen Auswirkungen des Einsatzes von Cloud-Lösungen im Rahmen seiner Governance der Digitalisierung und der Informationssysteme geprüft. Dies veranlasste ihn zur Bestätigung einer Strategie, die auf einer kontrollierten Nutzung ausgelagerter Dienste basiert, sofern diese ausreichende Garantien in Bezug auf Sicherheit, Datenschutz, Verfügbarkeit der Dienste und Kostenkontrolle bieten und gleichzeitig der Ausrichtung des Richtplans der Digitalisierung und der Informationssysteme entsprechen. Der Staatsrat achtet besonders darauf, dass sich die Daten in der Schweiz befinden und legt ein besonderes Augenmerk auf die mit ihrer Auslagerung verbundenen Risiken. So wurden im Rahmen von Projekten bei der gemäss Artikel 41 des Gesetzes über den Datenschutz (DSchG) durchgeführten Datenschutz-Folgenabschätzung die folgenden drei Risiken identifiziert:

- > Der Standort der Daten kann nicht rechtsverbindlich garantiert werden, was zu einem Kontrollverlust über sensible Informationen führen kann.
- > Die potenzielle Anwendung ausländischer Rechtsvorschriften, insbesondere des US Cloud Act, könnte ausländischen Behörden den Zugriff auf Daten ermöglichen, die sich im Besitz von Anbietern befinden, die diesen Rechtsvorschriften unterliegen.
- > Die Nutzung von Cloud-Diensten impliziert eine Auslagerung der Datenbearbeitung, was zu einer erhöhten Abhängigkeit vom Anbieter hinsichtlich Verwaltung, Sicherheit und Governance führt.

Um diese Risiken zu verringern, schränkt der Staat das Hosting bestimmter Kategorien besonders sensibler Informationen in der Cloud ein, macht den jeweiligen Anbietern spezifische vertragliche Vorgaben und sorgt dafür, dass die Steuerungs- und Kontrollmöglichkeiten über die ausgelagerten Bearbeitungsvorgänge gewahrt bleiben. Die Folgenabschätzungen werden zudem immer dann erneut überprüft, wenn die Entwicklung der Bearbeitungsvorgänge, der Technologien oder des regulatorischen Umfelds dies rechtfertigt.

In rechtlicher Hinsicht erfordert der Einsatz von Microsoft 365 besonderes Augenmerk auf die Vorgaben der Gesetzgebung zum öffentlichen Beschaffungswesen und zum Datenschutz, auf die Bedingungen für internationale Datenübermittlungen sowie auf die potenziellen Auswirkungen der für die Anbieter geltenden ausländischen Rechtsvorschriften.

In finanzieller Hinsicht entstehen durch die Nutzung von Microsoft 365 wiederkehrende Kosten für Lizenzen und damit verbundene Dienstleistungen, die mit rund 4,5 Millionen Franken zu veranschlagen sind. Mit einer allfälligen Migration auf alternative Lösungen sind jedoch keine nennenswerten Einsparungen zu erwarten, da sie ebenfalls

¹ Das ISDS-Konzept bildet die Grundlage für die Festlegung der Massnahmen für Informationssicherheit und Datenschutz (ISDS). Es zeigt die Restrisiken auf, die mit dem Betrieb des Systems und der Organisation verbunden sind (Quelle: www.hermes.admin.ch)

² Folgenabschätzung gemäss Art. 41 und 42 DSchG (SGF 17.1), nach den Vorgaben der zuständigen Behörde (<https://www.fr.ch/de/staat-und-recht/transparenz-und-datenschutz/datenschutzfolgenabschaetzung>)

erhebliche Investitionen in die Integration, die Begleitung bei der Umstellung, die Schulung, den Support und die Governance mit sich bringen würde.

In organisatorischer Hinsicht ist Microsoft 365 heute fest in die Arbeitsprozesse der Kantonsverwaltung und der Bildungseinrichtungen sowie in zahlreiche Fachanwendungen integriert. Jede wesentliche Änderung dieser Umgebung würde eine intensive Begleitung der Nutzenden, die Anpassung zahlreicher interner Prozesse sowie bestehender technischer Schnittstellen erfordern.

2.3 Alternativen und digitale Souveränität

Der Staatsrat ist sich bewusst, dass es effektiv Alternativen zu Microsoft 365 gibt. Er hält es daher für notwendig, die kritischen digitalen Abhängigkeiten des Staates weiter abzuklären und im Rahmen seiner Governance der Informationssysteme die realistischen Möglichkeiten zur Diversifizierung, Reversibilität und Stärkung der digitalen Souveränität zu evaluieren.

Der Staatsrat weist jedoch darauf hin, dass es diesbezüglich nicht darum gehen kann, einen Anbieter komplett durch einen Anbieter zu ersetzen. Eine effiziente digitale Souveränität zielt nicht darauf ab, technologisch autark zu sein, was in einem stark vernetzten digitalen Umfeld weder realistisch noch wünschenswert ist. Es geht vielmehr darum, die Wahlfreiheit zu bewahren, eine zu starke Abhängigkeit von einem einzelnen Anbieter zu vermeiden und sicherzustellen, dass bei Bedarf auf andere Lösungen umgestiegen werden kann.

In dieser Hinsicht tragen die Vielfalt von Lösungen und ihre bessere Reversibilität zur Risikobegrenzung bezüglich Datenschutz und zur Kontinuität öffentlicher Dienstleistungen bei.

Erfahrungen im In- und Ausland zeigen, dass eine Migration technisch möglich ist. Eine solche Umstellung ist jedoch mit grossen Herausforderungen verbunden:

- > Technische Komplexität: Im Gegensatz zu integrierten Suites wie Microsoft 365 basieren alternative Lösungen oft auf einer Zusammenstellung einzelner Komponenten, was mit einem erheblichen Integrationsaufwand verbunden ist.
- > Organisatorischer Aufwand: Die Einführung neuer Tools bringt tiefgreifende Veränderungen für die Nutzerinnen und Nutzer mit sich und erfordert umfangreiche Schulungs- und Begleitprogramme.
- > Interne und finanzielle Kapazitäten: Sich von einem Anbieter unabhängig zu machen, bedeutet, dass eine interne Lösung für einen Teil seiner bisherigen Verantwortlichkeiten gefunden werden muss. Dazu bräuchte es eine erhebliche Aufstockung der technologischen, finanziellen und personellen Ressourcen des Amtes für Informatik und Telekommunikation (ITA) und auch der Ressourcen für das Kompetenzzentrum Fritic für die Schulen des Kantons.
- > Gesamtkosten: Auch wenn gewisse alternative Lösungen als «Open Source» bezeichnet werden, heisst das nicht, dass sie gratis sind. Die Kosten für Entwicklung, Integration, Betrieb, Support und Governance müssen vollumfänglich berücksichtigt werden. Eine vollständige Umstellung könnte diesbezüglich mit sehr hohen Investitionen verbunden sein, ohne dass kurz- und mittelfristige Einsparungen garantiert wären.
- > IT-Sicherheit: Kein Schweizer Akteur ist in der Lage, so viel wie Microsoft in die Stärkung der Sicherheit seiner Produkte, Cloud-Dienste und Infrastrukturen zu investieren. So hat Microsoft im Jahr 2021 bekannt gegeben, über fünf Jahre 20 Milliarden US-Dollar in die Stärkung der Cybersicherheit zu investieren.
- > Aktive Rolle des Staates: Die Nutzung von «Open Source»-Lösungen impliziert, dass sich der Staat nicht auf die Rolle eines Konsumenten beschränkt, sondern zu einem aktiven Akteur wird (Beiträge, Entwicklung, Beteiligung an Communities), was einen Paradigmenwechsel darstellt.

Die Debatten über die digitale Souveränität konzentrieren sich häufig auf sichtbare Cloud-Dienste, insbesondere auf kollaborative Suites wie Microsoft 365, was allerdings ein unzureichender Ansatz sein kann, wenn er hauptsächlich auf einer Logik des Misstrauens gegenüber ausländischen Anbietern beruht. Auch bei Daten in sogenannten «souveränen» Umgebungen bleiben die wesentlichen Schichten der Informatikinfrastruktur in der Regel von Microsoft-Technologien abhängig: Windows, Azure, Identitätsdienste, Verwaltungstools oder Sicherheitsmechanismen.

Angesichts dieser technischen Realität wird mit einer Beschränkung der Überlegungen allein auf die Anwendungssouveränität von M365 ausser Acht gelassen, dass auch auf den unteren Infrastrukturebenen eine potenzielle Kontrolle ausgeübt wird. Wenn ein Technologieanbieter im Kern der Betriebssysteme, der Authentifizierung oder der Cloud präsent bleibt, geht die Frage nach dem potenziellen Zugriff auf Informationen weit über den blossen Perimeter der gehosteten Daten hinaus.

Dies zeigt die Grenzen von Ansätzen auf, die sich ausschliesslich auf die Datenlokalisierung oder Argwohn in rechtlicher Hinsicht beziehen. Eine Souveränität, bei der es sich lediglich um einen Wechsel des Hosting-Standorts handelt, bietet für sich genommen keine echte Garantie für Sicherheit oder Unabhängigkeit. Eine nachhaltige Strategie sollte vielmehr auf Resilienz, die Beherrschung der Kontrollmechanismen und die Diversifizierung technologischer Abhängigkeiten abzielen.

2.4 Aktionsplan und innovativer Ansatz

Angesichts der steigenden Anforderungen an Sicherheit, Compliance und Datenkontrolle wird ein Aktionsplan gestützt auf einen innovativen Ansatz für die digitale Souveränität unumgänglich. Bislang basierten Strategien zur Wahrung der Souveränität hauptsächlich auf der Datenlokalisierung – ein kostspieliger, komplexer und rechtlich unvollständiger Ansatz, da die genutzten Infrastrukturen oder Dienste weiterhin ausländischen Rechtsvorschriften unterliegen. Vor diesem Hintergrund erscheint operative Resilienz heute strategisch wichtiger als eine klassische Souveränität, die auf technologischer Isolation beruht. Ein neuer Ansatz bestünde nun darin, nicht mehr die Daten selbst zu verlagern, sondern die Kontroll- und Governance-Mechanismen, und zwar mithilfe vertrauenswürdiger Komponenten, die es ermöglichen, einen schweizerischen Rechtsrahmen auch innerhalb öffentlicher, privater oder hybrider Cloud-Umgebungen anzuwenden. Mit diesem Ansatz liessen sich die Kapazitäten der grossen Marktakteure nutzen und gleichzeitig Garantien für Kontrolle, Reversibilität und Unabhängigkeit wahren. Langfristig könnte diese Strategie die Entstehung eines vertrauenswürdigen digitalen Umfelds in der Schweiz fördern, das insbesondere von der Digitalen Verwaltung Schweiz getragen wird und Innovation, Neutralität und Nachhaltigkeit digitaler Dienste miteinander in Einklang bringt.

Der Staatsrat hält fest, dass auf Bundesebene und in mehreren Kantonen in Bezug auf die Problematik der Abhängigkeit von Microsoft-Lösungen und allgemeiner der digitalen Souveränität schon einiges unternommen wird. So hat etwa der Bund eine Machbarkeitsstudie zur Prüfung einer möglichen Open-Source-Alternative zu Microsoft 365 in Auftrag gegeben und treibt gleichzeitig die grossflächige Einführung dieser Lösung voran. Weiter haben sich auch verschiedene Kantone im Rahmen von parlamentarischen Vorstössen oder strategischen Arbeiten mit dieser Frage befasst, allerdings ohne dass bisher auch nur ein Gemeinwesen einen vollständigen Ausstieg aus den Microsoft-Lösungen eingeleitet hätte. Daran ist einerseits zu sehen, dass die Behörden über die Abhängigkeit von solchen Anbietern besorgt sind, und andererseits, dass diese Abhängigkeit systembedingt ist und einen vorsichtigen und pragmatischen Ansatz erfordert.

Jede Initiative, die auf eine echte digitale Souveränität abzielt, wäre angesichts der strategischen, technologischen und finanziellen Herausforderungen in Milliardenhöhe ohne eine umfassende Koordinierung auf Bundesebene undenkbar. Der Aufbau souveräner, resilienter und wettbewerbsfähiger Infrastrukturen geht weit über die Möglichkeiten isolierter Initiativen oder begrenzter finanzieller Mittel hinaus.

Dabei kommt der Digitalen Verwaltung Schweiz (DVS) eine zentrale Rolle bei der Festlegung gemeinsamer Ausrichtungen und Kapazitäten auf nationaler Ebene zu. Der Staatsrat engagiert sich hier bereits aktiv, und zwar sowohl interkantonal als auch auf Bundesebene, insbesondere durch seine Mitwirkung in den Führungsgremien der DVS, aber auch im Rahmen der vom Finanzdirektor des Kantons Freiburg präsidierten *Conférence latine des directeurs du numérique (CLDN)* und der vom Direktor des ITA geleiteten *Groupe numérique des cantons latins (GNCL)*, einer Vereinigung der IT-Verantwortlichen. Dementsprechend will der Staat Freiburg aktiv an der Umsetzung der *Swiss Government Cloud* mitwirken, mit dem Ziel, die öffentlichen digitalen Infrastrukturen gemeinsam zu nutzen, sie zu kontrollieren und ihre Resilienz zu gewährleisten.

Der Staatsrat hält schliesslich fest, dass die Diversifizierung der Lösungen zwar dazu beitragen kann, bestimmte Abhängigkeiten zu verringern, aber auch andere Risiken mit sich bringen kann, insbesondere in Bezug auf Kohärenz, Sicherheit, Produktivität und Service-Continuity.

Das Streben nach mehr digitaler Souveränität muss daher gegen die Anforderungen an Stabilität, Betriebssicherheit und Effizienz der öffentlichen Dienste abgewogen werden.

2.5 Fazit

Der Staatsrat hält es für notwendig, weiter strukturierte Überlegungen zu kritischen technologischen Abhängigkeiten, deren Entwicklung sowie zu realistischen Möglichkeiten der Diversifizierung und Reversibilität anzustellen. Er ist sich jedoch bewusst, dass eine vollständige Loslösung von der Abhängigkeit von Microsoft, insbesondere kurz- oder mittelfristig, angesichts der Anforderungen an Kontinuität, Sicherheit, Interoperabilität und Effizienz der öffentlichen Dienstleistungen keine realistische Option ist.

Er setzt deshalb auf einen pragmatischen Ansatz, der darin besteht:

- > die Herausforderungen der technologischen Abhängigkeiten und des Datenschutzes weiterhin immer im Blick zu behalten;
- > die Entwicklung des Marktes und alternativer Lösungen zu verfolgen;
- > dort, wo es zweckmässig ist, dem spezifischem Bedarf entsprechende diversifizierte, alternative oder ergänzende Lösungen zu nutzen;
- > in Abstimmung mit den Arbeiten auf Bundes- und interkantonaler Ebene die Abhängigkeiten von kritischen digitalen Lösungen weiter vertieft zu analysieren, um realistische und wirtschaftlich tragfähige Szenarien für Diversifizierung und Reversibilität zu identifizieren;
- > die aktive Mitwirkung des Kantons Freiburg bei den Initiativen im Rahmen der Digitalen Verwaltung Schweiz (DVS), der Conférence latine des directeurs du numérique (CLDN) und der Groupe numérique des cantons latins (GNCL) fortzusetzen.

Im Rahmen der bereits eingeleiteten Schritte wird der Staatsrat den innovativen Ansätzen für mehr Datenhoheit, bessere Governance und Kontrolle der Daten in öffentlichen, privaten oder hybriden Cloud-Umgebungen besondere Aufmerksamkeit schenken.

Der Staatsrat lädt den Grossen Rat ein, von diesem Bericht Kenntnis zu nehmen.