Kanton Obwalden

Regierungsrat

Sitzung vom: 26. Mai 2025
Beschluss Nr.: 364

Interpellation betreffend mit Open Source zu mehr digitaler Souveränität und Datenschutz?; Beantwortung.

Der Regierungsrat beantwortet

die Interpellation betreffend „Mit Open Source zu mehr digitaler Souveränität und Datenschutz?" (Nr. 54.25.04), welche von den Kantonsräten Martin Hug, Alpnach, und Gregor Jaggi, Sarnen, sowie 23 Mitunterzeichnenden am 20. März 2025 eingereicht wurde, wie folgt:

1. Gegenstand der Interpellation

Die Interpellanten halten fest, dass in den letzten Jahren zahlreiche öffentliche Verwaltungen im In- und Ausland einen Umstieg auf Open-Source-Software (OSS) versucht oder vollzogen hätten. Der Quellcode von OSS sei nicht verschlossen, sondern allen zugänglich und offengelegt, was die Transparenz der Datenverarbeitung erhöhe und sogar individualisierte Anpassungen und Weiterentwicklungen zulasse. Gründe für die Einführung von OSS in der öffentlichen Verwaltung seien unterschiedlich und würden vom Bemühen um Kostenreduktion bis hin zur Durchsetzung eigener Datensouveränität reichen. Ebenfalls könne die Abhängigkeit der öffentlichen Verwaltung von einzelnen Softwareanbietern reduziert werden und es werde eine schnellere Innovation bei IT-Anwendungen ermöglicht. Durch den öffentlich einsehbaren Quellcode werde auch die Sicherheit erhöht, da dieser von allen auf Schwachstellen geprüft und gegebenenfalls korrigiert werden könne. Im Bereich der Büroapplikationen bestünden zahlreiche Alternativen und Programme für jedes Bedürfnis, welche den käuflich zu erwerbenden nicht OSS-Programmen qualitativ gleichgestellt seien.

2. Hintergrund und fachliche Sichtweise zum Betrieb von OSS in der kantonalen Verwaltung

OSS bezeichnet Programme, deren Quellcode öffentlich zugänglich ist. Das bedeutet, dass jeder den Code einsehen, verändern und weiterverbreiten kann, sofern die Lizenzbedingungen eingehalten werden. Diese Offenheit fördert Transparenz und ermöglicht es Organisationen, die Software an ihre spezifischen Bedürfnisse anzupassen. Zudem erlaubt sie eine unabhängige Überprüfung der Funktionsweise, was das Vertrauen in die Software stärkt. OSS wird oft in gemeinschaftlichen Projekten entwickelt, bei denen Entwickler weltweit zusammenarbeiten. Diese kollaborative Entwicklung kann zu innovativen und qualitativ hochwertigen Lösungen führen.

OSS bringt viele Vorteile mit sich, insbesondere im Hinblick auf Unabhängigkeit, Anpassbarkeit und langfristige Nachhaltigkeit. Gleichzeitig ist der professionelle Einsatz von OSS im produktiven Verwaltungsumfeld mit spezifischen Herausforderungen verbunden, insbesondere wenn keine eigene Softwareentwicklung und nur eingeschränkte betriebliche Ressourcen zur Verfügung stehen.

2.1 Betriebsrealität im Informatikleistungszentrum Obwalden– Nidwalden (ILZ)

Das ILZ betreibt eine komplexe Applikationslandschaft mit rund 800 Applikationen und ca. 400 Servern, die mehrheitlich Linux-basiert sind. Aufgrund des Umfangs und der Vielfalt ist ein vollständig interner Betrieb und Unterhalt aller Systeme mit eigenem Personal nicht realisierbar. Viele Applikationen und Basisdienste werden in enger Zusammenarbeit mit externen Partnern betrieben, sei es im Rahmen von Wartungsverträgen, Supportvereinbarungen oder durch vollständiges Outsourcing einzelner Systeme.

2.2 Betriebliche Einschätzung durch das ILZ

2.2.1 Wartung und Weiterentwicklung

Ein wesentlicher Vorteil von OSS ist der offene Quellcode. Allerdings verpflichtet diese Offenheit Organisationen auch dazu, Verantwortung für die Wartung und Aktualisierung zu übernehmen. Anders als bei kommerziellen Anbietern, die Sicherheitsupdates garantieren und regelmässig bereitstellen, hängt die Qualität und Geschwindigkeit bei OSS stark von der jeweiligen Community oder vom gewählten Dienstleister ab.

Projekte mit starker Community (z. B. LibreOffice, GitLab, Kubernetes) sind zuverlässig gepflegt. Weniger verbreitete oder veraltete OSS-Projekte können Sicherheitslücken enthalten, die nicht zeitgerecht behoben werden. Ohne eigene Entwickler oder Spezialisten ist es nicht möglich, im Notfall selbst einzugreifen oder Anpassungen vorzunehmen. Daher ist beim Einsatz von OSS zwingend sicherzustellen, dass ein professioneller externer Wartungspartner zur Verfügung steht, der:

- Sicherheitsupdates zeitnah einspielt;
- einen definierten Lifecycle- und Patch-Prozess sicherstellt;
- verbindliche Service Level Agreements (SLAs) garantiert.

2.2.2 Cybersecurity

Im Bereich der Informationssicherheit ergeben sich bei OSS zwei konträre Sichtweisen:

- Einerseits erlaubt der offene Quellcode eine grössere Transparenz. Schwachstellen können offen geprüft, gemeldet und schneller behoben werden.
- Andererseits können Angreifer diese Offenheit ebenfalls nutzen, um gezielt Schwachstellen in schlecht gewarteten OSS-Installationen auszunutzen.

Ohne strukturierte Wartung, kontinuierliches Monitoring und proaktive Sicherheitsmassnahmen kann OSS ein erhebliches Cyberrisiko darstellen – insbesondere bei Systemen mit direkter Anbindung an das Internet.

Das ILZ betreibt heute ein mehrschichtiges Sicherheitsmodell mit regelmässigen Schwachstellenscans, Monitoring und Incident Response. OSS-Lösungen müssen in diese Sicherheitsarchitektur vollständig integriert werden können, inklusive:

- automatisiertem Patch-Management;
- Protokollierung und Auditing;
- Vulnerability Scanning;
- Möglichkeit zur schnellen Reaktion auf neue Bedrohungen.

Diese Anforderungen sind mit gängigen OSS-Lösungen grundsätzlich erfüllbar – allerdings nur, wenn sie durch erfahrene Dienstleister begleitet und regelmässig aktualisiert werden.

2.2.3 Integration und Support

Viele OSS-Lösungen bieten heute nicht den gleichen Grad an technischer Integration wie proprietäre Systeme grosser Anbieter. Der administrative Aufwand für Integration in bestehende Infrastruktur (z. B. Identity Management, Backup, zentrale Überwachung, Schnittstellen zu Drittsystemen) kann hoch sein.

Auch beim Support ist zu beachten: Es existieren für viele OSS-Lösungen keine 24/7-Supportangebote mit garantierten Reaktionszeiten, wie sie in einer Verwaltung mit hoher Verfügbarkeitsanforderung notwendig sind. Die Verfügbarkeit qualifizierter Dienstleister ist je nach Lösung unterschiedlich ausgeprägt.

Daher sollte OSS nur dort eingesetzt werden, wo langfristiger professioneller Support durch externe Partner sichergestellt werden kann oder wo Ausfälle nicht unmittelbar kritische Folgen haben.

2.3 Fazit aus betrieblicher Sicht (ILZ)

Der Einsatz von OSS in der kantonalen Verwaltung ist grundsätzlich möglich, aber an klare Bedingungen geknüpft:

- OSS darf nicht als „kostenloser Ersatz" für proprietäre Lösungen verstanden werden, sondern muss wie jede andere Software professionell betrieben, gewartet und unterstützt werden;
- ohne eigene Entwickler ist der Betrieb von OSS nur in Partnerschaft mit spezialisierten externen Dienstleistern verantwortbar;
- die Auswahl geeigneter OSS-Lösungen muss sicherheits- und wartungsorientiert erfolgen und durch ein strukturiertes Lifecycle- und Sicherheitsmanagement begleitet werden.

Das ILZ betreibt bereits heute eine differenzierte OSS-Strategie, die betriebliche und sicherheitstechnische Aspekte gleichwertig berücksichtigt und verbindliche Kriterien für Auswahl, Betrieb und Support von OSS-Systemen definiert.

3. Beantwortung der Fragen

3.1 Welche Lizenzgebühren werden kumuliert jährlich für Standardsoftware (Büroapplikationen, keine Fachanwendungen) und Betriebssysteme an welche Softwareentwicklern (z.B. Microsoft) im ILZ-Verbund und in der kantonalen Verwaltung ausgegeben (wichtigste Positionen für Obwalden)?

Das ILZ bezahlte für das Jahr 2024 für sämtliche Kunden folgende Lizenzgebühren für Standardsoftware und Betriebssysteme:

Anbieter	Kosten
Microsoft Standardsoftware M365 E5	1 082 000 Fr.
Microsoft Betriebssysteme Server	35 000 Fr.
Microsoft Datenbanken	79 300 Fr.
Oracle Datenbanken	23 000 Fr.

Die Kosten entsprechen den gesamten Lizenzkosten, die das ILZ für alle Kunden gegenüber den Lieferanten bezahlt. Der Kanton Obwalden bezahlt ca. 33 Prozent der Gesamtkosten.

3.2 Gemäss Medienberichten sind öffentliche Verwaltungen beim Einsatz von MS Office 365 stark abhängig vom Hersteller. Bei Microsoft-Cloudlösungen kann es immer sein, dass vertrauliche Daten im Ausland, z.B. in den USA, landen. "Faktisch hat immer Microsoft und letztendlich der amerikanische Staat Zugriff auf diese Daten". Wie sieht die Regierung die Problematik bezüglich Datenschutz?

Die Nutzung von Microsoft 365 in der kantonalen Verwaltung bringt unbestrittene betriebliche Vorteile, insbesondere im Hinblick auf Integration, Benutzerfreundlichkeit und Funktionsumfang. Gleichzeitig bestehen jedoch berechtigte Bedenken hinsichtlich des Datenschutzes und der Datensouveränität. Trotz vertraglich vereinbartem, lokalem Hosting in schweizerischen Rechenzentren bleibt Microsoft als US-amerikanisches Unternehmen unter dem Geltungsbereich des CLOUD Act verpflichtet, auf Anforderung US-Behörden Zugriff auf gespeicherte Daten zu

gewähren – auch ohne Wissen der betroffenen Organisation. Dies stellt insbesondere für sensible Verwaltungsdaten ein Risiko dar, das mit den Anforderungen des öffentlichen Datenschutzrechts nur schwer in Einklang zu bringen ist.

Neue digitale Zusicherungen von Microsoft (April 2025) adressieren diese Problematik: Mit der „EU Data Boundary" sollen Kundendaten vollständig in der EU/EFTA verarbeitet werden. Ergänzend bietet Microsoft Funktionen wie Customer Lockbox, Confidential Computing und verschlüsselten Zugriff mit eigenen Schlüsseln, um die Datenhoheit zu stärken. Diese Zusicherungen verbessern die Lage deutlich. Dennoch bleibt ein Restrisiko bestehen, da Microsoft weiterhin dem US-Recht unterliegt. Für besonders sensible Daten sind daher weiterhin gezielte Schutzmassnahmen oder alternative Lösungen vorzusehen. Der Regierungsrat prüft projektspezifisch und gestützt auf die fachliche Beurteilung des ILZ die Risiken und versucht diese mit gezielten Massnahmen zu reduzieren. Zuletzt erfolgte eine entsprechende Beurteilung mit der Einführung von M365-Diensten und dem Einsatz von MS Teams (Videokonferenzsystem und Dateiablagen in der Azure Cloud auf Servern von Microsoft in der Schweiz) im Rahmen der Corona-Pandemie mit Regierungsratsentscheiden am 7. April 2020 und 8. September 2020.

3.3 Auch beim Einsatz von künstlicher Intelligenz (KI) gelangen Daten automatisch zu den Softwareentwicklern. In welchen Bereichen erachtet die Regierung den Einsatz von KI als sinnvoll und wo kann dieser aus Datenschutzgründen bedenklich sein?

Künstliche Intelligenz bietet der öffentlichen Verwaltung erhebliches Potenzial, insbesondere zur Automatisierung repetitiver Aufgaben, zur Analyse grosser Datenmengen und zur Effizienzsteigerung in Prozessen mit hohem Standardisierungsgrad (z. B. Dokumentenklassifikation, Chatbots, Texterkennung). Der Nutzen ist unbestritten, wenn der Einsatz kontrolliert, transparent und zweckgebunden erfolgt.

Kritisch zu beurteilen ist der Einsatz von KI dort, wo personenbezogene oder vertrauliche Daten verwendet werden und unklar ist, wie diese durch proprietäre KI-Systeme weiterverarbeitet oder gespeichert werden. Bei Cloud-basierten KI-Modellen, insbesondere aus dem Ausland, besteht die Gefahr der unbeabsichtigten Datenweitergabe. Aus Sicht des Regierungsrats empfiehlt sich deshalb der bevorzugte Einsatz von lokalen oder Open-Source-basierten KI-Modellen, um die Kontrolle über Datenflüsse zu gewährleisten und den Datenschutz sicherzustellen. Der Regierungsrat hat deshalb bereits im Oktober 2023 ein entsprechendes Merkblatt erstellt, um die Nutzung von Online-KI-Generatoren verwaltungsintern zu regeln.

3.4 Wie sieht die Regierung die Chancen und Machbarkeit des Einsatzes von Open-Source-Software? Unabhängigkeit von einem Hersteller, Kosteneinsparungen, maximale Flexibilität, Hardwareplattform-Unabhängigkeit und Sicherheit gegenüber den vertrauten Lösungen der grossen Anbieter und der damit verbundenen Komfortzone bei der täglichen Arbeit der kantonalen Verwaltung?

Open-Source-Software bietet auf den ersten Blick viele Vorteile: Unabhängigkeit von einzelnen Herstellern, Kosteneinsparungen durch Wegfall von Lizenzgebühren, Flexibilität bei Anpassungen sowie Plattformunabhängigkeit. Gerade in Zeiten wachsender Anforderungen an Transparenz und digitale Souveränität ist das ein attraktives Konzept für öffentliche Verwaltungen.

In der Praxis zeigt sich jedoch, dass diese Vorteile stark von den betrieblichen Voraussetzungen abhängig sind. Eine Verwaltung ohne eigene Entwicklungsressourcen und mit beschränkten internen Betriebskapazitäten ist beim Einsatz von OSS in besonderem Mass auf kompetente externe Partner angewiesen – sowohl für die Systemintegration, den Unterhalt als auch für Support, Updates und Sicherheitspatches. Diese Dienstleistungen sind kostenpflichtig und können Einsparungen bei Lizenzgebühren teilweise oder ganz kompensieren.

Darüber hinaus bieten etablierte proprietäre Anbieter oft tief integrierte Komplettlösungen mit

langjähriger Roadmap, garantierten Supportverträgen, Schulungsangeboten und bewährten Sicherheitsstandards. Viele Open-Source-Alternativen erreichen zwar funktional ähnliche Ebenen, verlangen aber höhere technische Eigenverantwortung, was in einem regulierten und sicherheitskritischen Umfeld nicht immer tragbar ist.

Ein Wechsel zu OSS bedeutet daher nicht nur einen technologischen, sondern auch einen kulturellen Wandel. Komfort, Stabilität und Verlässlichkeit – wie sie von langjährig eingesetzten Produkten wie Microsoft Office erwartet werden – sind nicht automatisch gegeben. Schulungsaufwand, Umgewöhnung der Nutzerinnen und Nutzer sowie Integrationsaufwände in bestehende Systeme dürfen nicht unterschätzt werden.

Fazit: OSS kann bei sorgfältiger Auswahl, klarer Governance und verlässlichem Betriebspartner eine sinnvolle Ergänzung zur bestehenden Landschaft darstellen. Ein vollständiger Ersatz proprietärer Lösungen ist jedoch weder kurz- und mittelfristig realistisch noch pauschal ratsam. Vielmehr sollte OSS dort eingesetzt werden, wo funktionale Reife, Sicherheit und Support gewährleistet sind – und wo tatsächliche Vorteile gegenüber der bestehenden Lösung bestehen. Die Machbarkeit hängt dabei stark vom jeweiligen Anwendungsbereich, den verfügbaren OSS-Lösungen und der Umsetzungsbereitschaft innerhalb der Organisation ab. Der erfolgreiche Einsatz setzt eine klare Governance, Ressourcen für Wartung und Schulung sowie ein geeignetes Partnernetzwerk voraus.

3.5 In welchen Teilbereichen könnte man allenfalls eine Umstellung auf Open-Source-Software starten? Welche Bereiche sind allenfalls gar nicht für eine solche Umstellung geeignet?

Bereits heute wird beim ILZ gezielt OSS eingesetzt. Beispiele dafür sind:
- Keycloak für Identity Management;
- RabbitMQ als Messaging-Broker;
- PostgreSQL als Datenbanklösung;
- Linux als Serverbetriebssystem;
- Nextcloud, Draw.io, Inkscape, FreeMind, IrfanView, VLC Media Player etc. für verschiedenste Büro- und Spezialanwendungen;
- eine moderne Kubernetes-Infrastruktur für den Betrieb containerisierter Anwendungen, wie sie bei modernen Cloudanbietern eingesetzt werden.

Diese breite Nutzung zeigt, dass OSS bei entsprechender fachlicher Betreuung und Einbettung in den Betriebsstandard zuverlässig und sicher betrieben werden kann und wird. Ein weiterer Ausbau erscheint besonders in technischen Infrastrukturbereichen sinnvoll – etwa in den Feldern Orchestrierung, Automatisierung, Monitoring oder bei spezialisierten Fachanwendungen, wo sich OSS-Lösungen durch Innovationsgeschwindigkeit, Modularität und Community-Support auszeichnen.

Weniger geeignet für eine vollständige Umstellung auf OSS sind derzeit stark standardisierte Endanwenderprodukte (z. B. Office-Anwendungen, E-Mail, Kalender), bei denen Interoperabilität mit Drittsystemen, Benutzerkomfort, Supportverfügbarkeit und Akzeptanz eine zentrale Rolle spielen. Hier überwiegt aktuell noch der betriebliche Nutzen etablierter proprietärer Lösungen.

Fazit: OSS ist bereits ein tragender Bestandteil unserer Systemlandschaft. Ein gezielter, schrittweiser Ausbau in geeigneten Bereichen ist weiterhin möglich – sofern wirtschaftliche, sicherheitstechnische und betriebliche Mehrwerte klar erkennbar sind. Ein Wechsel von Softwarekomponenten und Anwendungen muss zudem die Vorgaben der Vereinbarung über die Zusammenarbeit in der Informatik (GDB 138.3) jedoch zwingend berücksichtigen und in Abstimmung mit den anderen beteiligten Körperschaften erfolgen.

Protokollauszug an:
- Mitglieder des Kantonsrats (samt Interpellationstext)
- Informatikleistungszentrum Obwalden – Nidwalden (ILZ)
- Finanzdepartement
- Staatskanzlei

Im Namen des Regierungsrats

Nicole Frunz Wallimann
Landschreiberin

KANTON OBWALDEN
REGIERUNGSRAT

Versand: 4. Juni 2025