

Luzern, 23. September 2025

ANTWORT AUF ANFRAGE**A 512**

Nummer: A 512
Protokoll-Nr.: 1036
Eröffnet: 08.09.2025 / Finanzdepartement

Anfrage Brunner Simone und Mit. über zentrale Risiken der Einführung von M365 in der Kantonsverwaltung und mögliche Alternativen

Vorbemerkung

Der digitale Wandel ist ein Kernelement der Kantonsstrategie. Die Verwaltung will und muss den digitalen Wandel aktiv gestalten, Prozesse digitalisieren, die Kommunikation verbessern und die Effizienz steigern. Mit der heute im Einsatz stehenden Bürosoftware *Office 2016* wird es zunehmend schwierig, diese Anforderungen zu erfüllen. Ausserdem wird sie vom Hersteller nicht mehr unterstützt. Die neue Software *Microsoft 365* (M365) ersetzt dieses alte System und ermöglicht der Verwaltung eine einheitliche, digitale Zusammenarbeit über die Abteilungs-, Departements-, und Kantonsgrenzen hinweg. Dadurch wird die Effizienz gesteigert, die Zusammenarbeit erleichtert und flexible Arbeitsweisen gefördert. Das Softwarepaket M365 besteht aus Applikationen, die in den kantonalen Rechenzentren betrieben werden (insbesondere die Office-Applikationen *Word, Excel und PowerPoint*) und aus Applikationen, die in der Cloud betrieben werden (insbesondere die Videokonferenz- und Kollaborationslösung *Teams*, das Nachfolge-Produkt von *Skype for Business*). M365 wird schon heute vom Bund und etlichen Kantonen genutzt und auch in der Privatwirtschaft breit eingesetzt. Eine Alternative zu M365, welche die gleiche Funktionsbreite zu einem ähnlichen Preis bietet und im selben Zeithorizont eingeführt werden kann, gibt es bis dato nicht. Unser Rat verfolgt aber fortlaufend die Entwicklung auf dem Markt.

Die Herausforderung ist, den Bedürfnissen der Bevölkerung sowie den Ansprüchen der Mitarbeitenden der kantonalen Verwaltung gerecht zu werden und gleichzeitig die hohen Anforderungen an den Datenschutz einzuhalten. Unser Rat ist sich dieses Spannungsfelds bewusst. Um sensible Daten zu schützen, werden diese weiterhin auf den lokalen Servern gespeichert und die cloudbasierten Applikationen eingeschränkt.

Dem Entscheid unseres Rates für M365 gingen mehrjährige, umfassende Abklärungen voraus. In einem umfangreichen Initialisierungsprojekt wurden die Anforderungen an eine rechtmässige Nutzung von M365 aufgelistet, mögliche Risiken identifiziert und entsprechende Massnahmen zur Reduktion definiert. Die Kritikpunkte des Datenschutzbeauftragten sowie die Hinweise des Kantonsgerichts wurden eingehend analysiert und in die Überlegungen einbezogen.

Die in den M365 Cloud Services bearbeiteten Daten werden nur in den Schweizer Rechenzentren der irischen Tochtergesellschaft von Microsoft gespeichert und ausschliesslich innerhalb der EU bearbeitet (nur in Ausnahmefällen kann es zu Datentransfers an die Microsoft-Muttergesellschaft in den Vereinigten Staaten kommen). Microsoft verpflichtet sich vertraglich zur sicheren, vertraulichen und zweckgebundenen Bearbeitung aller Daten des Kantons Luzern gemäss den Anforderungen des Schweizer Datenschutzrechts. Microsoft hat sich dazu verpflichtet, amerikanische Behörden auf den ordentlichen Weg der Rechtshilfe zu verweisen, sollten sie Daten herausverlangen. Darüber hinaus wurden mit Microsoft umfassende technische und organisatorische Massnahmen zur Sicherstellung von Datenschutz und Informationssicherheit vereinbart (u. a. Zugriffskontrollen, Protokollierung).

Nach Ansicht unseres Rates ist die Nutzung der M365 Cloud Services im beabsichtigten Umfang rechtskonform. Die im Tätigkeitsbericht des ehemaligen kantonalen Datenschutzbeauftragten geäusserte Ansicht, sie würde gegen Gesetze verstossen und gar in Grundrechte eingreifen, haben wir zur Kenntnis genommen, teilen sie aber nicht. Die Datenschutzaufsichtsbehörden vertreten zur Nutzung von Cloud-Diensten eine restriktive Haltung, die in juristischen Kreisen stark umstritten ist. Bislang hat keine Datenschutzaufsichtsstelle in der Schweiz der öffentlichen Verwaltung die Nutzung von M365 untersagt. Unser Rat steht kontinuierlich im Austausch mit der kantonalen Beauftragten für den Datenschutz, um eine für die Aufsichtsbehörde akzeptable Umsetzung von M365 sicherzustellen.

Zu Frage 1: Welche besonders schützenswerten oder vertraulichen Daten sollen Stand heute effektiv in der Microsoft-Cloud verarbeitet werden?

In der Cloud von Microsoft werden der E-Mail- und Kalender-Server, Speicherlaufwerke (*SharePoint Online, OneDrive*) sowie die Videokonferenz- und Kollaborationslösung *Teams* (das Nachfolge-Produkt von *Skype for Business*) betrieben. Die Datenklassifizierung legt verbindlich fest, welche Arten von Daten in welchen Anwendungen verarbeitet werden dürfen. Für geheime Informationen bestehen technische Restriktionen, sodass sie unter keinen Umständen in die Cloud gelangen können. Auch die E-Mail-Kommunikation unterliegt klaren Vorgaben. Gleichzeitig ist es für effizientes Arbeiten – sowohl innerhalb des Kantons als auch in der Zusammenarbeit nach aussen – unabdingbar, dass bestimmte Informationen zu definierten Zwecken per E-Mail geteilt werden. Entscheidend ist dabei ein hohes Bewusstsein im Umgang mit Daten sowie deren konsequente Bearbeitung und Ablage gemäss den Vorgaben der Datenklassifizierung und den entsprechenden Arbeitsanweisungen. Primäre Arbeitsinstrumente der kantonalen Verwaltung bleiben aber auch nach der Einführung von M365 die verschiedenen Fachanwendungen (z.B. im Steuerbereich) und das Geschäftsverwaltungssystem *CMI*. Insgesamt werden nur ungefähr 5 Prozent der kantonalen Daten in M365-Cloud-Diensten bearbeitet, rund 95% der Daten werden in Fachapplikationen bearbeitet und gespeichert. Die Daten der Fachapplikationen und auch jene der Office-Programme von M365 (Word, Excel, Powerpoint) werden nicht automatisch in die Cloud von Microsoft migriert.

Zu Frage 2: Wie beurteilt der Regierungsrat die Auswirkungen des US CLOUD Act auf die Vertraulichkeit dieser Daten, auch bei Speicherung in Schweizer Rechenzentren? Hat sich diese Beurteilung seit der Amtszeit der US-Regierung unter Donald Trump verändert?

Der US CLOUD Act gibt US-amerikanischen Strafverfolgungsbehörden das Recht, unter Umgehung der internationalen Rechtshilfe die Herausgabe von Kundendaten bei Microsoft zu verlangen, wenn dies der Aufklärung von schweren Straftaten (wie z.B. der Finanzierung von Terrorismus) dient. Das Restrisiko, dass dies Daten des Kantons Luzern betrifft, wird als sehr klein eingeschätzt. Die in den M365 Cloud Services bearbeiteten Daten werden nur in den Schweizer Rechenzentren der irischen Tochtergesellschaft von Microsoft gespeichert und ausschliesslich innerhalb der EU bearbeitet (nur in Ausnahmefällen kann es zu Datentransfers an die Microsoft-Muttergesellschaft in den Vereinigten Staaten kommen). Es ist nicht geklärt, ob auch solche Daten dem US CLOUD Act unterliegen. Microsoft hat sich ausserdem vertraglich dazu verpflichtet, amerikanische Behörden auf den ordentlichen Weg der Rechtshilfe zu verweisen, sollten sie Daten herausverlangen. Der Kanton Luzern reduziert das Risiko einer Datenherausgabe dadurch, dass die Clouddienste von M365 nicht für Daten verwendet werden dürfen, die von Interesse für US-amerikanische Strafverfolgungsbehörden sein könnten (vgl. auch Einführungen in der Vorbemerkung). Die Mitarbeitenden werden entsprechend geschult und sensibilisiert.

Der Amtsantritt von Donald Trump hat die Beurteilung des Risikos nicht wesentlich verändert. Es liegt nicht im Interesse von Microsoft, Kundendaten an US-amerikanische Behörden herauszugeben (siehe auch die Antwort auf Frage 9). Unser Rat berücksichtigt aber geopolitische Faktoren in der laufenden Risikobewertung und prüft Szenarien, um bei veränderten Rahmenbedingungen reagieren zu können.

Zu Frage 3: Welche konkreten "Exit-Szenarien" hat der Regierungsrat geprüft für den Fall, dass Microsoft-Dienste künftig datenschutzrechtlich, finanziell oder politisch nicht mehr tragbar sind?

Der Kanton Luzern hat (in Abstimmung mit der föderalen Zusammenarbeitsorganisation Digitale Verwaltung Schweiz) eine Exit-Strategie ausgearbeitet. Er beobachtet den Markt laufend im Hinblick auf alternative Lösungen und ist konzeptionell bereit für den Wechsel auf ein Alternativprodukt, falls Microsoft seine Verpflichtungen nicht mehr erfüllen kann oder will. Ausserdem wird der Kanton Luzern ein von Microsoft unabhängiges Backup der in M365 bearbeiteten Daten implementieren, um jederzeit handlungsfähig zu bleiben. Im Rahmen der Exit-Strategie wurden verschiedene Szenarien und Gründe entwickelt für einen Ausstieg aus Microsoft-Produkten, die strategischer, rechtlicher, finanzieller oder technischer Natur sind.

Zu Frage 4: In ihrer Antwort auf die Anfrage A 238 von Misticoni Fabrizio schreibt die Regierung, dass «Der Kanton Luzern die Situation am Markt im Hinblick auf mögliche Alternativen zu M365 beobachtet». Wie findet diese Beobachtung statt und zu welchem Ergebnis ist die Regierung seither gekommen?

Die Beobachtung des Marktes findet im Rahmen der kontinuierlichen Aktualisierung der Exit-Strategie statt. Bisher ist unser Rat der Auffassung, dass kein Alternativprodukt die Vorteile von M365 in punkto Interoperabilität, Kollaboration und Sicherheit annähernd erreicht und die Alternativprodukte entweder ähnliche Restrisiken aufweisen wie M365, oder sie andere Risiken erzeugen würden.

Zu Frage 5: Inwiefern wäre der Kanton Luzern bereit, in enger Zusammenarbeit mit den Gemeinden, Kantonen und dem Bund (sprich mit dem Verbund "Digitale Verwaltung Schweiz") ein "Cloud-Ökosystem" für die Verwaltung zu prüfen, das den spezifischen Anforderungen der öffentlichen Hand gerecht wird (analog den Plänen des IT-Rates in Deutschland)?

Im Rahmen der Digitalen Verwaltung Schweiz gehen Bund, Kantone und Gemeinden die interdisziplinären Fragestellungen der Cloudnutzung ganzheitlich an, unter Einbezug von Zivilgesellschaft, Politik, Wirtschaft und Wissenschaft. In diesem Zusammenhang ist auch die Swiss Government Cloud (SGC) zu erwähnen. Das Bundesamt für Informatik und Telekommunikation (BIT) baut zwischen 2025 und 2032 eine neue, auf die Anforderungen und Bedürfnisse des Bundes zugeschnittene Hybrid-Multi-Cloud-Infrastruktur auf, von der auch die Kantone und Gemeinden profitieren sollen.

Zu Frage 6: Wie wird das laufende Risikomanagement durchgeführt, wer ist beteiligt und wie werden neue Entwicklungen (z. B. geopolitische Risiken oder EU-Recht) einbezogen?

Das Risikomanagement für den Betrieb von M365 erfolgt im Rahmen des kantonalen Risikomanagements in enger Zusammenarbeit mit den zuständigen Fachstellen. Die Risiken werden laufend überwacht, regelmässig auditiert und bei relevanten Veränderungen, wie geopolitischen Entwicklungen oder neuen regulatorischen Vorgaben, neu bewertet. Bei der Einführung neuer Produkte oder Funktionen von M365 wird jeweils eine erneute Datenschutz-Folgenabschätzung durchgeführt, wie in § 7a des kantonalen Datenschutzgesetzes (SRL Nr. 38) vorgesehen. Dabei wird die Stellungnahme der kantonalen Datenschutzaufsicht eingeholt, um sicherzustellen, dass datenschutzrechtliche Risiken frühzeitig erkannt und adressiert werden. Parallel dazu werden Optionen zur Stärkung der betrieblichen Resilienz und zur Reduktion der Abhängigkeit vom Anbieter geprüft, um die Handlungsfähigkeit des Kantons auch bei veränderten Rahmenbedingungen zu wahren.

Zu Frage 7: Welche internen oder externen Gutachten oder Rechtsbeurteilungen wurden zur Unterstützung des M365-Projekts eingeholt? Werden diese den Kommissionen sowie dem Parlament zugänglich gemacht?

Im Projekt wurde eine Rechtsgrundlagenanalyse erstellt. Ausserdem wurden die Auswirkungen auf den Datenschutz in einer Datenschutzfolgenabschätzung untersucht, die dem kantonalen Datenschutzbeauftragten vorgelegt wurde. Unser Rat ist dazu bereit, den zuständigen Kommissionen Einblick zu gewähren.

Zu Frage 8: Wie beurteilt der Kanton das Risiko von Datenschutzlücken oder Uneinheitlichkeiten im Datenschutzniveau aufgrund der Eigenständigkeit der Gemeinden in IT-Fragen? Welche Massnahmen werden ergriffen, um dennoch einheitliche Standards bei der Einführung von M365 zu gewährleisten?

Die Gemeinden sind in der Organisation ihrer Informatik eigenständig und fallen nicht in den Verantwortungsbereich der kantonalen Verwaltung. Der kantonalen Verwaltung fehlen die

Ressourcen, um Gemeinden diesbezüglich zu unterstützen. Die Gemeinden werden – wie die kantonale Verwaltung – von der kantonalen Datenschutzbeauftragten beaufsichtigt und haben die Möglichkeit, sich von ihr beraten zu lassen. Ausserdem soll, voraussichtlich diesen Herbst, der Verein «Digitale Gemeinden Luzern» gegründet werden, der die Luzerner Gemeinden in Digitalisierungsfragen unterstützen soll.

Zu Frage 9: Auf welcher Grundlage wurde das Risiko eines Datenmissbrauchs als "klein" eingestuft, trotz möglicher Rechtsverstösse?

Das Risiko eines aktiven, vertragswidrigen Missbrauchs der Daten durch Microsoft selbst wird als gering eingeschätzt, da ein solches Verhalten im Widerspruch zu den wirtschaftlichen Interessen des Unternehmens stünde. Unabhängig davon bestehen jedoch strukturelle Risiken, die sich aus der extraterritorialen Anwendung des US CLOUD Act, aus geopolitischen Entwicklungen oder aus unbeabsichtigten technischen oder organisatorischen Schwachstellen ergeben können. Diese Risiken werden in der laufenden Sicherheits- und Risikoanalyse berücksichtigt und in den Schutzmassnahmen, den Schulungen sowie den Überwachungsmechanismen abgebildet.