Thurgau

Der Regierungsrat des Kantons Thurgau an den Grossen Rat

Frauenfeld, 24. Februar 2026
Nr. 100

24	EA 95	243

Einfache Anfrage von Kenny Greber, Linda Hess und Patrick Siegenthaler vom 17. Dezember 2025 „Einführung M365 und Datenschutz sowie digitale Souveränität“

Beantwortung

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Frage 1: Entscheidungsgrundlage/Rechtsgrundlage und Cloud Act: Auf welcher Grundlage hat der Regierungsrat die Einführung von Microsoft 365 beschlossen und damit die Sicherheit erlangt, dass die Einführung von M365 mit Blick auf den US Cloud Act und das Thurgauer Datenschutzgesetz (TG DSG) vollständig vereinbar ist? (Falls vorhanden, bitte Gutachten beilegen)

Auf der Basis der bestehenden Rechtsgrundlagen und der unter Beizug externer Spezialisten durchgeführten Risikoanalyse kam der Regierungsrat 2023 zum Schluss, dass Microsoft 365 (M365) mit technischen und organisatorischen Massnahmen zur Minimierung der Restrisiken zugelassen werden kann. Der Entscheid war das Resultat eines längeren Prozesses (inkl. Regierungsseminar), in welchem der Regierungsrat alle Departemente, die Staatskanzlei sowie den kantonalen Datenschutz- und Öffentlichkeitsbeauftragten einbezogen hat und sich von einer spezialisierten Anwaltskanzlei beraten lassen hat. Diese hat die rechtliche Machbarkeit in einem Bericht bestätigt. Weil zum Teil Rückschlüsse auf relevante Informationen im Bereich der IT-Sicherheit möglich sind, wird auf die Veröffentlichung dieser Unterlagen verzichtet.

Mittlerweile haben die meisten kantonalen Verwaltungen M365 eingeführt oder befinden sich in diesem Prozess. Auch angesichts der geopolitischen Entwicklungen wurde vom Amt für Informatik (AFI) im Herbst 2025 eine erneute externe Überprüfung in Auftrag gegeben mit dem Ziel, etwaigen Handlungsbedarf zu identifizieren, der sich seit der Freigabe der M365 Online Services im Jahr 2023 ergeben hat. Das Schlussfazit der

Überprüfung lautet wie folgt: „Die Analyse der rechtlichen, vertraglichen und technisch-organisatorischen Entwicklungen im Zeitraum von März 2023 bis Dezember 2025 hat gezeigt, dass die Grundlagen für den Einsatz von Microsoft 365 durch die Kantonale Verwaltung Thurgau weiterhin stabil sind und sich in der Tendenz verbessert haben.

Zusammenfassend lässt sich festhalten, dass die im Bericht vom 22. März 2023 gezogene Schlussfolgerung der rechtlichen Machbarkeit auch per 31. Dezember 2025 uneingeschränkt Bestand hat. Die seither erfolgten Entwicklungen, insbesondere die Etablierung der EU Data Boundary durch Microsoft, das Swiss-U.S. Data Privacy Framework und der neue DVS-Rahmenvertrag[1] mit Microsoft, haben die Rechtssicherheit für den Betrieb der M365-Dienste weiter gestärkt. Das Restrisiko von Behördenzugriffen aus dem Ausland wird weiterhin als äusserst gering und durch die getroffenen Massnahmen als angemessen mitigiert beurteilt.

Es bestehen somit aus rechtlicher Sicht weiterhin keine Hinderungsgründe für die Nutzung der M365-Onlinedienste für Personendaten, einschliesslich besonders schützenswerter Personendaten, sowie für Informationen, die dem Amtsgeheimnis unterliegen.

Wir empfehlen dem AFI TG, die Entwicklungen weiterhin periodisch zu beobachten und die Gewährleistung der Datensicherheit laufend sicherzustellen. Eine nächste formelle Überprüfung der Rechtslage wird per Ende 2028 empfohlen."

Frage 2: Datenklassifizierung und -speicherung: Welche speziellen Kategorien von Daten (z.B. Personaldossiers, Sozialdaten, Steuerdaten oder Daten der Führungsstäbe) werden explizit vom Einsatz in den M365-Cloud-Diensten ausgeschlossen?

M365 wird in der Kantonalen Verwaltung Thurgau (KVTG) zu Informations-, Kollaborations- und Kommunikationszwecken eingesetzt. Sämtliche Kernprozesse werden jedoch weiterhin über das zentrale Geschäftsverwaltungssystem Fabasoft oder spezifische Fachapplikationen abgewickelt und in lokalen Rechenzentren gespeichert. Diese zentralen IT-Systeme wurden durch die Einführung der M365-Plattform nicht tangiert. Dies betrifft alle in der Frage angeführten Beispiele wie Personaldossiers, Sozialdaten, Steuerdaten oder Daten der Führungsstäbe. Diese Massnahme erachtet der Regierungsrat als wirkungsvoller als die Einführung eines umfangreichen Datenklassifizierungssystems, das in der Praxis schwierig umsetzbar wäre.

Frage 3: Zugriffskontrolle und Verschlüsselung: Welche technischen, organisatorischen und vertraglichen Massnahmen werden ergriffen (z.B. Verschlüsselung mit vom Kanton selbst verwalteten Schlüsseln), um zu verhindern, dass Microsoft

---

[1] Rahmenvertrag der Digitalen Verwaltung Schweiz (DVS).

oder US-Behörden unverschlüsselten Zugriff auf kritische Daten des Kantons erhalten? (Bitte insbesondere Angaben zum Datenstandort, zur Verschlüsselung, zu Zugriffsberechtigungen sowie vor allem dazu, wie sichergestellt wird, dass die Weisung – keine vertraulichen bzw. besonders schützenswerten Daten in der Cloud zu speichern – von den Mitarbeitenden konsequent eingehalten wird.)

Es werden die durch Microsoft eingesetzten Standards verwendet. Der US-Konzern hat die Gegebenheiten im europäischen behördlichen Kontext verstanden und orientiert sich im eigenen Interesse daran. Es wurden zum Beispiel Rechenzentrumsstandorte innerhalb der Schweiz bereitgestellt, in denen exklusiv die Daten von Schweizer Behörden und Unternehmen bearbeitet werden. Die Daten verlassen unser Land nicht. Ausserdem verpflichtet sich Microsoft vertraglich zur Einhaltung der einschlägigen europäischen und schweizerischen Datenschutz- und Sicherheitsanforderungen.

In der M365-Cloud kommt ein mehrschichtiges Sicherheits- und Verschlüsselungskonzept zum Einsatz. Als zentrale Verschlüsselung von gespeicherten Daten dient AES-256. Beim bidirektionalen Datentransfer zwischen den kantonalen Rechenzentren und den M365-Cloud-Rechenzentren kommen die gängigen Transportverschlüsselungs-Standards zum Einsatz. Microsoft-Teams-Sitzungen sind End-to-End verschlüsselt (AES-256 + SRTP), wobei Microsoft keinen Zugriff auf Inhalte hat.

Durch das umfassende Vertragswerk, das von der Digitalen Verwaltung Schweiz (DVS) mit Microsoft ausgehandelt wurde und für sämtliche Behörden in der Schweiz zur Anwendung kommt, ist sichergestellt, dass Microsoft nur in Fällen von betrieblicher Notwendigkeit (z.B. in Supportfällen) auf Daten der KVTG Zugriff nimmt. Darin verpflichtet sich Microsoft explizit dazu, keinerlei Daten weiterzugeben und bei allfälligen behördlichen Zugriffsversuchen (z.B. gestützt auf den Cloud Act) sämtliche möglichen Rechtsmittel zu ergreifen.

Die Wirksamkeit dieser Massnahmen ist massgeblich von der sachgerechten Konfiguration, der Nutzung sicherheitsrelevanter Funktionen und der Einbindung in die jeweiligen organisatorischen Prozesse abhängig. Deshalb nimmt das AFI in verschiedenen Bereichen laufend professionelle Unterstützung durch ausgewiesene externe Partner in den Bereichen IT-Security, Datenschutz und der vertraglichen Situation mit Microsoft in Anspruch.

Frage 4: Kosten und Alternativen (Vendor Lock-in): Wurde eine umfassende Kosten-Nutzen-Analyse unter Berücksichtigung der Gesamtbetriebskosten (TCO) über fünf Jahre im Vergleich zu datenschutzkonformen Open-Source-Alternati-

ven, Schweizer Cloud Lösungen oder On-Premises-Lösungen durchgeführt, um die langfristige Abhängigkeit (Vendor Lock-in) vom Anbieter zu minimieren?

Auf dem Markt existiert faktisch keine Alternative zu M365 für grosse Organisationen, die dem Funktionsumfang in dieser Homogenität als ein reibungslos funktionierendes Gesamtprodukt und nahtlosem Zusammenspiel der einzelnen Komponenten auch nur annähernd gleichkommt.

Open-Source-Alternativen gibt es für nahezu alle Einzelkomponenten von M365. Die Integration und der reibungslose Betrieb dieser Komponenten in ihrem Zusammenspiel würden grosse Organisationen wie die KVTG in der Praxis vor unverhältnismässige Herausforderungen stellen. Das fehlende Zusammenspiel von Open-Source-Produkten mit den rund 600 in der KVTG eingesetzten Fachanwendungen würde eine enorme Herausforderung darstellen, da sich alle Lieferanten mit Integrationsforderungen für ihre Produkte konfrontiert sähen. Die dafür notwendigen Schnittstellen wären mit sehr hohen Kosten und Risiken für einen stabilen Betrieb verbunden.

Zudem wäre die Bedienung von Open-Source-Alternativen für die Vielzahl der Benutzerinnen und Benutzer in der KVTG nicht zumutbar. Die weite Verbreitung der Produkte von Microsoft hat den Vorteil, dass der grösste Teil der Benutzerinnen und Benutzer mit entsprechendem Vorwissen ausgestattet ist, was den täglichen Umgang stark erleichtert und ein rasches Einarbeiten und effizientes Arbeiten ermöglicht. Deshalb wurde für die KVTG der Gesamtservice bei Microsoft eingekauft. Eine umfassende TCO-Analyse wurde nicht durchgeführt.

Frage 5: Rechtliche Lücke und Souveränitätsauftrag: Der Regierungsrat hat den Entscheid im Rahmen seiner Exekutivkompetenz gefasst. Welche konkrete Verordnung oder gesetzliche Grundlage müsste der Grosse Rat erlassen oder anpassen, um die Auslagerung von besonders schützenswerten Personendaten und Daten der kantonalen Führung (vgl. Frage 2) an Cloud-Dienste, die ausländischen Gesetzgebungen wie dem US Cloud Act unterliegen, rechtsverbindlich zu verbieten oder zwingend an die Voraussetzung der uneingeschränkten Datensouveränität zu knüpfen?

Das Betriebssystem M365 ist ein reines Hilfsmittel, das der KVTG dazu dient, ihren gesetzlich geregelten Tätigkeiten nachzugehen. Zu bestimmen, welche Hilfsmittel in der KVTG eingesetzt werden, liegt in der Kompetenz der Exekutive.

Wie bei der Beantwortung von Frage 2 erläutert, wird M365 in der KVTG zu Informations-, Kollaborations- und Kommunikationszwecken eingesetzt, während alle geschäftsrelevanten Abläufe über das zentrale Geschäftsverwaltungssystem Fabasoft oder spezifische Fachapplikationen lokal abgewickelt werden. Mit diesen Massnahmen

wird sichergestellt, dass sensitive Daten nicht systematisch in M365-Applikationen verarbeitet werden.

Das kantonale Recht kennt bisher keine umfassende Datenklassifizierung. Das Gesetz über den Datenschutz (TG DSG; RB 170.7) befasst sich einzig mit Personendaten. Ein normiertes umfangreiches Datenklassifizierungssystem würde das Risiko eines sehr hohen administrativen Aufwands im täglichen Betrieb bergen.

Der Regierungsrat stellt mit aller Deutlichkeit klar, dass ein genereller Ausschluss für die Nutzung von M365 nur für Daten mit einem sehr hohen Schutzbedarf in Frage kommen kann. Dazu gehören beispielsweise Informationen zur Landesverteidigung, Zeugenschutzinformationen oder geheime Daten. Zu den besonders schützenswerten Daten gehört nach § 3 Abs. 2 TG DSG z.B. „die religiöse, weltanschauliche Ansicht oder politische Betätigung". Streng genommen ist damit bereits eine Parteizugehörigkeit einer Person als besonders schützenswerter Datensatz einzustufen. E-Mail-Programme, Kollaborationswerkzeuge und Dateiablagen von M365 für diese Datenkategorie überhaupt nicht zu verwenden, wäre in der Praxis nicht umsetzbar.

Der Präsident des Regierungsrates

Der Staatsschreiber

DER REGIERUNGSRAT · DES KANTONS THURGAU ·