KANTON
LUZERN

Regierungsrat

Luzern, 24. September 2024

ANTWORT AUF ANFRAGE A 238

Nummer: A 238
Protokoll-Nr.: 1047
Eröffnet: 09.09.2024 / Finanzdepartement

Anfrage Misticoni Fabrizio und Mit. über die Datensicherheit und die Datensouveränität bei der Einführung von «Microsoft 365»

Die Dienststelle Informatik (DIIN) ersetzt ab 2025 die heute im Einsatz befindliche Büro-Software Microsoft Office 2016 durch Microsoft 365 (M365). M365 wird lokal und in der Cloud betrieben:

- lokal: die sogenannten «Office-Anwendungen» (Word, Excel, Powerpoint, OneNote und Outlook) sind wie bisher auf den Geräten der Anwenderinnen und Anwender installiert und die darin bearbeiteten Daten werden in den Rechenzentren des Kantons bearbeitet;
- in der Cloud: die sogenannten «M365 Cloud Services» werden in der Cloud, das heisst in den Schweizer Rechenzentren von Microsoft, betrieben. Es handelt sich dabei um Speicherlaufwerke für Zusammenarbeit und Datenaustausch (SharePoint Online) sowie die Videokonferenz-, Telefonie- und Datenaustauschlösung Teams (das Nachfolge-Produkt von Skype for Business). Zu einem späteren Zeitpunkt soll auch der E-Mail- und Kalender-Server in der Cloud betrieben werden (Exchange Online).

Primäre Arbeitsinstrumente der kantonalen Verwaltung bleiben auch nach der Einführung von M365 die verschiedenen Fachanwendungen (z.B. im Steuerbereich) und das Geschäftsverwaltungssystem (GEVER). Im Zusammenspiel mit den lokal installierten Office-Anwendungen ermöglichen sie, Dokumente mit besonders sensiblem Inhalt lokal zu bearbeiten und auszutauschen. Für weniger sensible Daten kann die Verwaltung zukünftig von den verbesserten Kollaborationsfunktionen der M365 Cloud Services profitieren.

Zu Frage 1: Wie sieht der Zeitplan für die Einführung von Microsoft 365 in der kantonalen Verwaltung aus?

M365 wird im Kanton Luzern schrittweise eingeführt. Ab Sommer 2025 sollen die Applikationen Word, Excel, PowerPoint, OneNote, Outlook und die Telefonie mit Teams eingeführt werden. Ab 2026 ist die Einführung der Teams-Kollaborationsfunktionen vorgesehen.

Zu Frage 2: Wie wird eine Einführung und Umsetzung von M365 im Einklang mit den Datenschutzgesetzen (kantonal, national) gewährleistet?

Die kantonale Verwaltung untersteht dem kantonalen Datenschutzgesetz (KDSG, SRL Nr. 38). Die Anforderungen des Datenschutzgesetzes an einen rechtskonformen Betrieb von M365 wurden untersucht und die Einführung wird juristisch begleitet. Der Kanton Luzern orientiert sich an etablierten Standards für einen datenschutzkonformen Betrieb von Cloud Services.

Zu Frage 3: Wie wird zwischen verschiedenen Datenarten (beispielsweise besonders schützenswerten Daten) differenziert, insbesondere bezüglich der Ablage auf verschiedenen Clouds? Welche Services bleiben lokal installiert, damit die Datenbearbeitung in kantonalen Rechenzentren erfolgt? Welche Richtlinien bzw. Handlungsanweisungen wird es für den Umgang mit sensiblen Daten geben?

Die Office-Anwendungen Word, Excel, PowerPoint, OneNote und Outlook bleiben auch nach der Einführung von M365 auf den kantonalen Arbeitsgeräten installiert. Die damit bearbeiteten Dokumente werden auf den Arbeitsgeräten lokal bearbeitet und in den Rechenzentren des Kantons gespeichert. In der Cloud, das heisst in den Rechenzentren von Microsoft, werden zukünftig die M365 Cloud Services betrieben. Diese umfassen Speicherlaufwerke für Zusammenarbeit und Datenaustausch (SharePoint Online) und die Videokonferenz-, Telefonie- und Datenaustauschlösung Teams (das Nachfolge-Produkt von Skype for Business). Zu einem späteren Zeitpunkt soll auch der E-Mail- und Kalender-Server in der Cloud betrieben werden (Exchange Online).

Primäre Arbeitsinstrumente der Verwaltung bleiben auch nach der Einführung von M365 die verschiedenen Fachanwendungen und das Geschäftsverwaltungssystem (GEVER). Dort erfolgt die langfristige Speicherung und Archivierung der Daten. Die M365 Cloud Services können künftig zum Austausch von Informationen oder zur Kollaboration (z.B. gemeinsames zeitgleiches Arbeiten an einem Dokument) verwendet werden. Zu diesem Zweck dürfen Informationen bis und mit der Klassifizierungsstufe «vertraulich» (vgl. § 8 der Informatiksicherheitsverordnung, SRL Nr. 26b) respektive Personendaten bis und mit «besonders schützenswert» (vgl. § 2 Abs. 2 Kantonales Datenschutzgesetz [KDSG], SRL Nr. 38) in M365-Cloud Services bearbeitet werden. Für «geheim» klassifizierte Informationen und für Informationen, die aus rechtlichen Gründen nicht in einer Cloud bearbeitet werden dürfen, ist die Nutzung von M365-Cloud Services nicht gestattet. Die Mitarbeitenden werden entsprechend sensibilisiert, geschult und technisch unterstützt.

Zu Frage 4: Wie wird die Datensicherheit und die Datensouveränität bei nicht durch die kantonale Verwaltung gehostete Daten gewährleistet? Wo werden diese Daten bearbeitet und geschützt? Wo ist der Gerichtsstand für allfällige Verfahren? Wie steht es mit der Rechtsstaatlichkeit bei der Möglichkeit eines Zugriffs durch ausländische Behörden?

Mit jeder Auslagerung von Informatikdienstleistungen (auch «IT Outsourcing») geht ein gewisser Kontrollverlust über die ausgelagerten Daten einher. Das kantonale Informatikgesetz verlangt deshalb von der Verwaltung bei Auslagerungen gewisse vertragliche, technische und

organisatorische Schutzmassnahmen (siehe §§ 13 ff. Informatikgesetz, SRL Nr. 26). Diese werden auch bei der Nutzung von M365 vorgesehen. Microsoft verpflichtet sich vertraglich zur sicheren, vertraulichen und zweckgebundenen Bearbeitung aller Daten des Kantons Luzern gemäss den Anforderungen des Schweizer Datenschutzrechts. Der Kanton sichert ausserdem die in der Cloud von Microsoft gespeicherten Daten mit einem eigenen, von Microsoft unabhängigen Back-up, so dass sie jederzeit verfügbar bleiben (und auch ohne die M365 Cloud Services weiterbearbeitet werden können).

Die in den M365 Cloud Services bearbeiteten Daten werden nur in den Schweizer Rechenzentren von Microsoft gespeichert und ausschliesslich innerhalb der EU bearbeitet (wobei in Einzelfällen Datentransfers in die USA vorbehalten bleiben).

Der Gerichtsstand für Streitigkeiten im Zusammenhang mit der Bearbeitung von Personendaten ist Zürich.

Zur letzten Frage siehe Antwort zu Frage 5.

Zu Frage 5: Es besteht die Gefahr, dass besonders schützenswerte Personendaten oder auch Steuerdaten von Bürgerinnen und Bürgern in den USA landen können. Mit welchen Ausführungsbestimmungen wird dem vorgebeugt?

US-amerikanische Strafverfolgungsbehörden können von Microsoft – basierend auf US-amerikanischem Recht (US CLOUD Act) und unter Umgehung der Verfahren der internationalen Rechtshilfe – die Herausgabe von Kundendaten verlangen, wenn dies der Aufklärung von schweren Straftaten (insbesondere Terrorismus) dient. Unser Rat schätzt das Risiko einer solchen Herausgabe derzeit als klein ein. Nach unserem Kenntnisstand wurde der CLOUD Act noch nie gegen eine Schweizer Behörde anstelle eines Rechtshilfegesuches eingesetzt. Ausserdem hat Microsoft sich vertraglich dazu verpflichtet, amerikanische Behörden auf den ordentlichen Weg der Rechtshilfe zu verweisen. Trotzdem dürfen die Cloud Services von M365 nicht für Daten verwendet werden, die von Interesse für US-amerikanische Strafverfolgungsbehörden sein könnten. Die Mitarbeitenden werden entsprechend geschult und sensibilisiert.

Zu Frage 6: Wie beurteilt die Regierung grundsätzlich den Status des Kantons Luzern in Bezug auf Datensouveränität?

Unter Datensouveränität wird die selbstbestimmte Kontrolle über Erhebung, Speicherung, Nutzung und Bearbeitung der eigenen Daten verstanden. Auch nach der Einführung von M365 behält der Kanton Luzern ein hohes Mass an Datensouveränität. Bei jedem Outsourcing von Informatikdienstleistungen ergreift die kantonale Verwaltung die erforderlichen technischen, organisatorischen und rechtlichen Schutzmassnahmen, um die grösstmögliche Kontrolle über ihre Daten zu behalten.

Zu Frage 7: In anderen Kantonen und auf nationaler Ebene haben sich Datenschutzbeauftragte wohlwollend-kritisch zur Einführung von M365 geäussert. Wie wurde der Luzerner Datenschutzbeauftragte in die geplante Einführung miteinbezogen? Falls Empfehlungen gemacht wurden: Wie wurden diese umgesetzt? Sind sie der Öffentlichkeit zugänglich?

Das Finanzdepartement hat zur geplanten Einführung von M365 eine Datenschutz-Folgenabschätzung (§ 7a KDSG) durchgeführt und den Beauftragten für den Datenschutz zu den Ergebnissen konsultiert. Der Beauftragte für den Datenschutz hat verschiedene Empfehlungen gemacht, von denen ein Teil umgesetzt wird. Die Stellungnahme des Beauftragten für den Datenschutz wird nicht veröffentlicht, da sie sicherheitsrelevante Informationen enthält.

Zu Frage 8: Wie begleitet der Kanton und/oder der Datenschutzbeauftragte Gemeinden, welche ebenfalls M365 einführen wollen oder bereits eingeführt haben?

Die Gemeinden sind in der Organisation ihrer Informatik eigenständig. Der kantonalen Verwaltung fehlen die Ressourcen, um Gemeinden diesbezüglich zu unterstützen. Gemäss seinem aktuellen Tätigkeitsbericht hat der Beauftragte für den Datenschutz im vergangenen Jahr verschiedene Gemeinden bei der Einführung von M365 begleitet.

Zu Frage 9: Beabsichtigt die Regierung die Schaffung einer gesetzlichen Grundlage für den Einsatz von M365 als neuen digitalen Arbeitsplatz, ähnlich wie beispielsweise der Kanton Zürich?

Der Betrieb von Informatiksystemen als Mittel zur Erfüllung von Verwaltungsaufgaben ist eine administrative Hilfstätigkeit. Administrative Hilfstätigkeiten können ohne besondere gesetzliche Grundlage durch einen privatrechtlichen Vertrag auf Dritte übertragen werden. Ausserdem verfügt der Kanton Luzern mit den §§ 13 ff. Informatikgesetz bereits über eine allgemeine gesetzliche Grundlage für die Auslagerung von Informatikdienstleistungen. Die Schaffung einer spezifischen gesetzlichen Grundlage für den Einsatz von M365 ist daher nicht erforderlich. Auch der Bund und die meisten anderen Kantone sehen keine Notwendigkeit, für den Einsatz von M365 neue Gesetzesgrundlagen zu schaffen.

Zu Frage 10: Die weltweiten Ausfälle vom 19. Juli 2024 (Fehlerhaftes Update bei Crowdstrike-Falcon auf Microsoft Systemen) haben exemplarisch aufgezeigt, wie problematisch die Abhängigkeit von einem einzigen Monopol-Anbieter sein kann. Dies betrifft zum einen die Funktionsfähigkeit aber auch die ökonomische Abhängigkeit. Welche strategischen Planungen zur Diversifikation und Absicherung sind geplant?

Betreffend Funktionsfähigkeit weisen die M365 Cloud Services eine hohe Verfügbarkeit auf (z.B. 99,9% im zweiten Quartal 2024). Ausserdem ist Microsoft mit seinen grossen personellen Ressourcen schneller in der Lage, die Funktionsfähigkeit eines Cloud-Services wiederherzustellen, als es die Dienststelle Informatik bei vergleichbaren, selbst betriebenen Anwendungen wäre. Eine Diversifizierung im Sinne eines parallelen Einsatzes von mehreren gleichartigen Produkten (z.B. M365, Google Workspace und Open-Source-Produkten wie Libre Office) wäre ausserdem sehr teuer.

Die Abhängigkeit der gesamten westlichen Welt von einigen wenigen IT-Grosskonzernen wie Microsoft beurteilt auch unser Rat kritisch. Der Kanton Luzern hat, zusammen mit den anderen Kantonen und dem Bund, die Organisation «Digitale Verwaltung Schweiz» gegründet. Diese ist unter anderem damit beauftragt, für Bund, Kantone und Gemeinden möglichst vorteilhafte ökonomische Konditionen mit Microsoft auszuhandeln. Ausserdem verfolgt der Kanton Luzern die Situation am Markt im Hinblick auf mögliche Alternativen zu M365.