Stadt Luzern
Stadtrat
Hirschengraben 17
6002 Luzern
www.stadtrat.stadtluzern.ch

T 041 208 82 11
stadtrat@stadtluzern.ch

Antwort auf die Interpellation 85

Konsequenzen aus dem Bericht des kantonalen Datenschutzbeauftragten

Adrian Häfliger und Monika Weder namens der GRÜNE/JG-Fraktion vom 10. Juni 2025
StB 947 vom 17. Dezember 2025

Wurde anlässlich der Ratssitzung vom 29. Januar 2026 beantwortet

A. Ausgangslage

Der Interpellant und die Interpellantin verweisen auf den Tätigkeitsbericht 2024 des damaligen kantonalen Datenschutzbeauftragten (DSB) und auf die Stellungnahme der neuen kantonalen Datenschutzbeauftragten zur geplanten Einführung von Microsoft M365 in der kantonalen Verwaltung. Der Bericht enthalte drei zentrale Problemfelder und formuliere entsprechende Handlungsempfehlungen. Da die Stadt Luzern bereits Microsoft M365 einsetzt, ersuchen der Interpellant und die Interpellantin den Stadtrat um die Beantwortung von Fragen.
Der Interpellant und Interpellantin beziehen sich auf drei vom Datenschutzbeauftragten genannte Problemfelder. Zur Beantwortung der Fragen legt der Stadtrat in den folgenden einleitenden Bemerkungen vorab die Grundlagen zu den angesprochenen Bereichen (1. Digitale Souveränität / Vendor Lock-in, 2. Informationelle Selbstbestimmung, 3. Datensicherheit und Risikomanagement) dar.

B. Einleitende Bemerkungen

In der «Digitalstrategie und Smart City Luzern» (B+A 29 vom 30. August 2021) wurde festgehalten, dass die Stadt betreffend die digitale Transformation wegweisend sein will. Dazu gehört auch der Einsatz von zeitgemässen Arbeitsinstrumenten wie die M365-Umgebung. Dabei soll die Zusammenarbeit durch moderne Technologien und Arbeitsformen erleichtert und die Einbindung von Anspruchsgruppen und externen Partnern gefördert werden.

Ebenfalls einleitend zu erwähnen ist, dass der «Ethikbeirat Smartes Luzern» zuhanden des Stadtrates eine Stellungnahme zur Interpellation 85 eingereicht hat. Inhaltlich stützt sich der Ethikbeirat auf die Aussagen des DSB zur digitalen Souveränität im Tätigkeitsbericht 2024. Viele Datenschützerinnen und Datenschützer in der Schweiz äussern in einer Resolution Bedenken gegen die Nutzung von US-Cloud-Services, wie u. a. Microsoft 365, durch Behörden. Sie weisen darauf hin, dass die Bearbeitung von sensiblen Daten das Amtsgeheimnis gefährde und die Datenhoheit einschränke. Die Berner Fachhochschule hat ein Projekt gestartet, das die Schaffung eines staatlichen Zentrums für digitale Souveränität zum Ziel hat. Daran beteiligen sich mehrere private IT-Unternehmen sowie auch verschiedene Behörden auf unterschiedlichen föderalistischen Ebenen.

1. Digitale Souveränität / Vendor Lock-in

Es gibt keine einheitliche Definition, was unter digitaler Souveränität zu verstehen ist. Der Bundesrat definiert die digitale Souveränität wie folgt: «Digitale Souveränität bedeutet, als Staat über die erforderliche Kontroll- und Handlungsfähigkeit im digitalen Raum zu verfügen, um die Erfüllung staatlicher Aufgaben sicherzustellen» (Bericht des Bundesrates vom 26. November 2025, Digitale Souveränität der

Schweiz). Staatliche Aufgaben lassen sich ohne digitale Hilfsmittel nicht erfüllen. Dabei gilt es zu beachten, dass es kaum staatliche digitale Infrastruktur gibt. Die Kontroll- und Handlungsfähigkeit der Verwaltung ist deshalb per se begrenzt. Gleichwohl muss es Ziel aller Verwaltungseinheiten sein, ihre Abhängigkeiten von externen Dienstleistern zu kennen, zu begrenzen und im Ernstfall handlungsfähig zu bleiben. Digitale Souveränität bedeutet somit, die Kontrolle über Daten, Infrastrukturen und Kernprozesse zu behalten und externe Dienstleister bewusst zu wählen oder zu wechseln. Diesem Anspruch stellt sich auch die Stadt Luzern, wie nachfolgend ausgeführt wird.

In den letzten 25 Jahren hat sich die ICT-Landschaft grundlegend verändert. Während früher viele Unternehmen und Verwaltungen individuelle Informatiklösungen für ihre Prozesse entwickelten, setzen sie heute überwiegend auf Standardprogramme und auf eine harmonisierte IT-Systemlandschaft.

Seit Mitte der 2000er-Jahre hat sich das Cloud-Computing rasant etabliert: Anstatt Programme oder Daten auf eigenen Geräten zu speichern oder in lokalen Rechenzentren zu betreiben, werden sie auf leistungsfähigen Servern in Rechenzentren von grossen Anbietern wie Microsoft, Google oder Amazon ausgeführt. Diese Betriebsart bietet zahlreiche Vorteile:
- Es fallen keine hohen Investitionen in eigene Hardware und Rechenzentren an.
- Die Kosten werden planbarer durch monatliche Gebühren.
- Die Wartung und Sicherheit liegen beim Anbieter, ebenso regelmässige Aktualisierungen.
- Programmänderungen und Sicherheitsaktualisierungen sind schnell für alle Nutzenden verfügbar.
- Der Zugriff auf die Programme ist über das Internet von überall und performant auf der Welt möglich.
- Die Anzahl Benutzerinnen und Benutzer einer Anwendung kann jederzeit erhöht oder reduziert werden.

Die breite Verfügbarkeit von Cloud-Diensten führte in den frühen 2010er-Jahren dazu, dass viele Hersteller von Fachanwendungen und Standardprogrammen auf dieses Modell umstellten. Lizenzen werden nicht mehr für den Betrieb in den unternehmenseigenen Rechenzentren verkauft. Die Hersteller betreiben die Programme in eigenen Rechenzentren oder in den Rechenzentren der grossen Cloud-Anbieter. Sie vermieten die notwendigen Lizenzen und damit den Zugriff auf die Programme nur während der Vertragsdauer. Im Fachjargon nennt man dieses Bereitstellungsmodell «Software-as-a-service» (SaaS). Viele Anbieter stellen ihre Programme inzwischen ausschliesslich in dieser Form bereit.

Die Stadt Luzern hat diese Entwicklung früh erkannt und sich 2020 bei der Überarbeitung der IT-Strategie entschieden, künftig für Fachanwendungen auf SaaS zu setzen. Zurzeit nutzt die Stadt Luzern über 130 Fachanwendungen von mehr als 100 verschiedenen Lieferanten. Rund ein Drittel dieser Anwendungen wird nicht mehr in den eigenen Rechenzentren betrieben.

Auch im Bereich der Büroprogramme oder der Büroautomation hat der Trend schnell Einzug gehalten. Die weltweit am weitesten verbreitete Office-Suite von Microsoft (MS Office) wurde bereits 2013 als Abo-Modell angeboten. Mit der Version 2016 wurden immer mehr Funktionen in die cloudbasierte Version (Office 365) ausgelagert. Seit 2020 werden die gekauften und lokal installierten Office-Versionen (dauerhaft lizenziert) nur noch minimal gepflegt. Die Innovation findet nur noch in den Abonnements-versionen (Cloud-Services) statt. Neue Funktionen wie die Integration von künstlicher Intelligenz werden nur in den Cloud-Versionen zur Verfügung gestellt.

Ab 2020 hat Microsoft die Office365-Suite in «Microsoft 365» (kurz M365) umbenannt und als cloudbasierte Produktivitätsplattform M365 ausgebaut, die einiges mehr an Funktionalitäten bietet als die klassischen Office-Anwendungen. Microsoft will den Fokus auf die ganze Arbeitsplattform mit allen inzwischen integrierten Werkzeugen (insbesondere OneDrive, Teams, Planner, Sicherheitsfunktionen, Geräteverwaltung, KI-Funktionen) legen. Die Stadt Luzern hat ab 2021 von Office 2016 auf die Version M365 gewechselt und das Projekt «Azzurro» zum Roll-out der neuen Produkte gestartet.

M365 gilt heute in vielen Unternehmen und Verwaltungen als De-facto-Standard für eine umfassende und moderne Office- und Zusammenarbeitsumgebung. Es vereint Office-Anwendungen wie Word, Excel und PowerPoint mit Cloud-Speicher, Kommunikationsprogrammen und Sicherheitsfunktionen in einer

einheitlichen Suite. Früher brauchte man dafür viele verschiedene Programme, heute ist alles in einem Paket enthalten. Ein weiterer Vorteil ist die leichte Zusammenarbeit, der Datenaustausch und die Prozessautomatisierung. Mit M365 können mehrere Personen gleichzeitig an einem Dokument arbeiten, egal ob sie nebeneinander im Büro sitzen oder zu Hause arbeiten. Dateien lassen sich teilen, kommentieren und gemeinsam bearbeiten. Auch Besprechungen über Teams lassen sich spontan starten. Gerade in Zeiten von Homeoffice und mobil-flexibler Arbeit ist das ein entscheidender Vorteil. Ein grosser Vorteil ist auch die Sicherheit. Microsoft investiert viel Geld in den Schutz seiner Cloud-Anwendungen. Dadurch sind Daten oft besser geschützt, als wenn Firmen eigene Server betreiben. Funktionen wie Virenschutz, Schutz vor Hackerangriffen und regelmässige Sicherheitsupdates sind automatisch integriert. Zudem sind viele Arbeitsabläufe und Fachanwendungen in Verwaltungen bereits eng mit Microsoft-Produkten verknüpft. Viele Fachanwendungen setzen Windows, Outlook oder SharePoint voraus. Würde man alles auf andere Systeme umstellen, müssten viele Prozesse und Schnittstellen neu entwickelt werden. Dies wäre ein enormer Aufwand und würde viel Zeit und Geld kosten.

Für Verwaltungen in der Schweiz bietet der Markt heute keine vergleichbaren Alternativen zu M365. Es ist vertraut, sicher, weit verbreitet und eng mit vielen Fachanwendungen verknüpft. Ein Wechsel auf andere Systeme wäre technisch möglich, aber mit grossem Aufwand und hohen Kosten verbunden. Allen diesen Vorteilen stehen auch Nachteile und Risiken gegenüber, wie die Abhängigkeit von einer grossen Softwareanbieterin, Risiken bei der Bearbeitung von Personendaten (u. a. grössere technische Angriffsfläche, Auslandsbezug und mangelnde Durchsetzbarkeit von Rechten), eine erzwingbare Herausgabe von Daten an US-amerikanische Behörden sowie eine fehlende, echte Alternative (vgl. dazu nachfolgende Ausführungen zu einzelnen Risiken). Ein Wechsel von einem privatwirtschaftlichen Anbieter zu einem anderen löst das Grundproblem der Abhängigkeit nicht. Der Einsatz von Open-Source-Software allein bietet keine Garantie für digitale Souveränität. Eine zukunftsfähige Lösung erfordert ein Betriebsmodell, das Funktionalität, Sicherheit und Stabilität gewährleistet. Die Stärkung der digitalen Souveränität ist ein komplexer Prozess, der eine enge Zusammenarbeit zwischen verschiedenen Ebenen der öffentlichen Verwaltung in der Schweiz erfordert, nämlich zwischen dem Bund, den Kantonen und den Gemeinden. Diese Zusammenarbeit ist notwendig, um die hohen Kosten, die mit der Stärkung der digitalen Souveränität verbunden sind, tragbar zu machen und um Lösungen zu entwickeln, die effektiv, nachhaltig und skalierbar sind.

Die Stadt Luzern hat sich bewusst dafür entschieden, auf Cloud-Services zu setzen und insbesondere auf M365 zu wechseln. Die vom Stadtrat beschlossene IT-Strategie sieht seit 2020 ausdrücklich eine umfassende Nutzung von Cloud-Services für Applikationen und Services wie M365 vor («Cloud first»). Mit diesem Entscheid wurde das Abhängigkeitsrisiko im Rahmen einer Güterabwägung bewusst eingegangen. Ein weitgehender oder vollständiger Rückzug aus Cloud-Services (sog. «Exit-Strategie») ist infolgedessen derzeit nicht vorgesehen.

Den möglichen negativen Folgen der Abhängigkeit wird in der Stadt Luzern insbesondere mit zwei Massnahmen entgegengetreten: einerseits durch die Gewährleistung der Datensouveränität sowie andererseits durch die Erarbeitung von Ausstiegsszenarien.

Datensouveränität bedeutet, dass die Stadtverwaltung jederzeit und unabhängig vom Cloud-Service-Provider (insbesondere bei US-Anbietern) Zugang zu ihren wesentlichen Daten behält und diese – wenn auch mit erheblichem Aufwand – weiter nutzen kann. Dies wird erreicht, indem die innerhalb des Cloud-Services bearbeiteten Daten periodisch auf andere bzw. stadteigene IT-Systeme kopiert werden.

Ausstiegsszenarien umfassen Analysen und operative Konzepte, die dazu dienen, auf einen Wechsel zu einem anderen Cloud-Service-Provider, auf einen Technologiewechsel oder andere wesentliche Änderungen vorbereitet zu sein. Die Erarbeitung von Ausstiegsszenarien aus M365 ist komplex, aufwendig und nicht kurzfristig zu bewerkstelligen. Dabei müssen verschiedenste Aspekte berücksichtigt werden, angefangen bei der Beschaffung von Ersatzsystemen (Hardware und Software), der Herauslösung und Re-Integration von verbundenen Fachapplikationen, über die Migration der Daten,

die Aufrechterhaltung des Datenschutzes und der Informationssicherheit bis hin zur Schulung und Befähigung der Anwenderinnen und Anwender.
Beide Massnahmen – sowohl die Datensouveränität wie auch die Erarbeitung von Ausstiegsszenarien – sind integraler Bestandteil der stadtinternen und verbindlich einzuhaltenden Vorgaben für alle Projekte, welche die Nutzung eines Cloud-Services beinhalten, folglich auch für die Einführung von M365 (siehe dazu die Ausführungen im Abschnitt «Datensicherheit und Risikomanagement»).

Von einem Ausstiegsszenario zu unterscheiden ist ein plötzlicher, unvorhergesehener Ausfall bzw. eine Nichtverfügbarkeit von M365. Dies kann aus technischen Gründen geschehen oder wenn Microsoft in vertragsverletzender Weise den Zugang zu M365 sperren würde. Ein solcher Ausfall könnte je nach Dauer und Umfang eine hohe Tragweite für die Stadtverwaltung haben.
Der Umgang mit solchen und anderen aussergewöhnlichen Situationen oder Notfällen ist Inhalt des städtischen Business Continuity Managements (BCM). Teil davon ist, dass die Dienstabteilung Zentrale Informatikdienste (ZID) innert bestimmten Fristen und in reduziertem Umfang kritische Systeme und Daten als Notlösung bereitstellen und nach Beseitigung des Ausfalls wieder in den Normalbetrieb überführen kann.

2. Informationelle Selbstbestimmung

Das Grundrecht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) schützt die Privatsphäre. Jede Person soll grundsätzlich selbst bestimmen können, welche Daten über sie erhoben, gespeichert, verwendet oder weitergegeben werden. Soll dieses Recht eingeschränkt werden – weil der Staat zur Erfüllung seiner Aufgaben Daten seiner Bürgerinnen und Bürger braucht –, ist dafür wie bei jedem Grundrechtseingriff eine gesetzliche Grundlage notwendig. Weiter muss sich ein Grundrechtseingriff auf ein öffentliches Interesse stützen und verhältnismässig sein.

Das Datenschutzrecht konkretisiert das Grundrecht auf informationelle Selbstbestimmung und gewährleistet, dass die Datenbearbeitung die Persönlichkeit einer Person nicht verletzt. So werden die Anforderungen an die gesetzliche Grundlage und der Prozess der Interessenabwägung in den Datenschutzgesetzen von Bund und Kantonen konkretisiert.

Ein Prinzip des kantonalen Datenschutzrechtes ist, dass Personendaten nur für die gesetzliche Aufgabe bearbeitet werden dürfen, für die sie erhoben wurden (vgl. § 4 f. Kantonales Gesetz über den Schutz von Personendaten vom 2. Juli 1990; Kantonales Datenschutzgesetz, KDSG; SRL Nr. 38). Die Nutzung von M365 führt indessen zu keiner zusätzlichen oder neuen Datenbearbeitung innerhalb der bestehenden gesetzlichen Aufgaben. Mit der Nutzung von M365 werden die gleichen Daten mit neuen digitalen Hilfsmitteln bearbeitet. Die Bearbeitung von Daten mit M365 stellt aber eine Auslagerung der Datenbearbeitung an Dritte dar. Dies ist zulässig, wenn die gesetzlich definierten Vorgaben eingehalten werden (Auftragsdatenbearbeitung; § 6 Abs. 2 KDSG). Damit wird den Risiken begegnet, die mit einer Auslagerung der Datenbearbeitung verbunden sind.

Mit der Bearbeitung der Personendaten durch Angestellte privater (ausländischer) Firmen können folgende Risiken verbunden sein: Verlust direkter Kontrolle, grösserer Kreis von Akteuren und Subunternehmen (noch mehr Menschen, die Zugang zu den Daten haben), unterschiedliche Interessenlagen (private Unternehmen verfolgen in erster Linie ökonomische Interessen), grössere technische Angriffsfläche, Auslandsbezug und mangelnde Durchsetzbarkeit von Rechten.

Dabei ist indessen zu beachten, dass auch bei der Bearbeitung von Personendaten von Mitarbeitenden der Verwaltung Risiken bestehen. Fehlerhafte Datenbearbeitung kann wie folgt entstehen: unabsichtliche Fehlbearbeitung (falsches Erfassen von sensiblen Daten, Verwechslung von Dossiers, fehlerhafte Weiterleitung, falsches Einscannen, Zuordnen oder Ablegen), unzureichende Einhaltung von IT-Sicherheitsvorgaben (Passwörter unsicher aufbewahren, Phishing, Verwendung von USB-Sticks, Dokumente offen liegen lassen, Bildschirme nicht sperren) oder durch unzureichende Sensibilisierung (mangelhafte Kenntnis der Datenschutzregeln).

Mit technischen, organisatorischen sowie vertraglichen Massnahmen müssen diese Risiken so weit minimiert werden, dass sie akzeptiert werden können. Kann mit den Massnahmen sichergestellt werden, dass die Dritten die Personendaten nur so bearbeiten, wie es die Behörden selbst dürfen, ist eine Auslagerung der Datenbearbeitung im Grundsatz zulässig (vgl. § 6 Abs. 2 KDSG).

Zu diesen Massnahmen zählt bei M365 insbesondere die EU Data Boundary. Mit dieser wird sichergestellt, dass die Daten in M365 nur innerhalb der EU/EFTA bearbeitet werden. Die Datenspeicherung erfolgt grundsätzlich nur auf Schweizer Rechenzentren. Zudem wird mit einer vertraglichen Massnahme der Schutz der Daten vor der Herausgabe an Behörden ergänzt. Diese Massnahmen sind von der Stadt Luzern umgesetzt. Die weiteren technischen und organisatorischen Massnahmen sind im nachfolgenden Abschnitt näher erläutert.

3. Datensicherheit und Risikomanagement

Das Management von Datenschutz- und Informationssicherheitsrisiken ist in der Stadtverwaltung institutionalisiert und orientiert sich an der Norm ISO/IEC 27001.[1] Hierzu hat der Stadtrat die Ziele, Grundsätze und Zuständigkeiten in Form einer verbindlichen Weisung (Informationssicherheitspolitik) geregelt. Dabei werden Ziel- und Interessenkonflikte proaktiv vermieden, indem die Verantwortlichkeiten zwischen strategischer/taktischer und operativer Informationssicherheit innerhalb der Stadtverwaltung organisatorisch getrennt sind. Für die strategische/taktische Informationssicherheit ist die Fachstelle digitale Sicherheit und Privatsphäre (Fachstelle DSP) zuständig. Diese ist der Dienstabteilung Digital zugeordnet, welche ihrerseits Teil der Bildungsdirektion ist. Die Fachstelle DSP definiert die detaillierten Vorgaben an den Datenschutz und die Informationssicherheit («DSP-Standards[2]») und überprüft deren Einhaltung in Projekten und im Betrieb. Die operative Umsetzung der Vorgaben, vor allem in technischer und IT-betrieblicher Hinsicht, liegt primär in der Verantwortung der Zentralen Informatikdienste ZID. Die ZID sind eine Dienstabteilung der Finanzdirektion und somit organisatorisch getrennt von der Fachstelle DSP.

Für jedes Digitalisierungs- und Informatikvorhaben der Stadtverwaltung werden durch die Fachstelle DSP anhand einer Risikoabschätzung die jeweils anwendbaren DSP-Standards festgelegt. Das damit zu erreichende Schutzniveau wird als Basisschutz bezeichnet. In der Datenschutzgesetzgebung wird hierfür der Begriff «technische und organisatorische Massnahmen» verwendet.
Vorhaben wie die Einführung von M365, welche Cloud-Services beinhalten und bei denen vertrauliche Daten bearbeitet werden sollen, ziehen höhere Risiken nach sich. Um diese Risiken zu minimieren, müssen strengere und cloudspezifische Massnahmen umgesetzt werden. Dieses Schutzniveau wird stadtintern als «Basisschutz Cloud+» bezeichnet.
Die städtische M365-Umgebung mit ihren zugehörigen Teilsystemen wie Teams, Exchange Online, SharePoint Online und OneDrive muss das Schutzniveau «Basisschutz Cloud+» erreichen.

Betrifft ein Vorhaben die Bearbeitung von besonders schützenswerten Personendaten, wird ergänzend eine Datenschutz-Folgenabschätzung gemäss kantonaler Datenschutzgesetzgebung durchgeführt. Hierbei stützt sich die Stadt Luzern auf die Vorgaben und Hilfsmittel, die von der DSB publiziert sind. Mit diesem Instrument wird zusätzlich geprüft, ob trotz des Basisschutzes noch hohe Risiken für die Verletzung der Persönlichkeit und Privatsphäre für betroffene Personen bestehen.
Für die Nutzung von M365 wurde eine Datenschutz-Folgenabschätzung durchgeführt. Diese hat ergeben, dass mit der Umsetzung von «Basisschutz Cloud+» zusammen mit den rechtlichen und vertraglichen Massnahmen für betroffene Personen die Risiken angemessen adressiert werden können.

Diese beiden Schritte (Festlegung und Prüfung der anwendbaren DSP-Standards, Datenschutz-Folgenabschätzung) sind fester Bestandteil der städtischen Projektmanagement-Methodik und müssen von allen Projekten eingehalten werden. Dies gilt auch für die Einführung von M365.

[1] ISO/IEC 27001: Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme – Anforderungen.
[2] Den DSP-Standards liegen die Normen ISO/IEC 27002 und 27701 zugrunde. Diese wurden mit den Vorgaben der kantonalen Datenschutzgesetzgebung ergänzt.

Die DSB hebt die konsequente Ausrichtung der DSP-Standards an den genannten Normen sowie die Festlegung des «Basisschutzes Cloud+» − der über die gesetzlichen Mindestanforderungen hinausgehe − positiv hervor.

Zur Sicherheit der städtischen M365-Umgebung
M365 kann nicht per se als sicher oder unsicher bezeichnet werden. Die Sicherheit bezieht sich immer auf eine bestimmte Umgebung von M365. Die Stadt Luzern hat eine solche M365-Umgebung bei Microsoft «gemietet» bzw. lizenziert und ist – wie jede andere «Mieterin» auch – selbst für die sichere Konfiguration, den sorgsamen Betrieb und die sicherheitsbewusste Nutzung verantwortlich.
Die Umsetzung von «Basisschutz Cloud+» für die städtische M365-Umgebung beinhaltet eine Vielzahl von Massnahmen. Einige der wichtigsten Massnahmen sind
- Strenge, sicherheitszentrierte Konfiguration der M365-Umgebung;
- Sicherheitsverifikation mit unabhängigen Penetrationstests;
- Zuverlässige Identifikation von Anwenderinnen und Anwendern;
- Schulung und Sensibilisierung der Mitarbeitenden;
- Zugang nur von ausdrücklich zugelassenen Notebooks, Smartphones und anderen Geräten;
- Verschlüsselte Übermittlung und Speicherung der Daten;
- Klassifizierung und Kennzeichnung von Daten;
- Einsatz von zusätzlichen Schutzfunktionen gegen Schadsoftware und Cyberattacken (MS Defender);
- Überwachung von Systemereignissen auf Anzeichen für Cyberattacken (Cyber Defence Center);
- Alarmierung und Intervention bei einer Cyberattacke (Security Operations Team und Notfallorganisation ZID);
- Datenzugriff durch Microsoft-Mitarbeitende nur bei Supportfällen und nur nach organisatorischer und technischer Freigabe durch ZID («Customer Lockbox»);
- Steuerung von Freigabe- und Zugriffsberechtigungen;
- Verwaltung von Gastzugriffen;
- Löschen von nicht mehr benötigten Daten;
- Sicherung und Wiederherstellung der Daten über einen grösseren Zeitraum hinweg (Cloud-Back-up);
- Von Microsoft unabhängige Kopie der Daten unter vollständiger Kontrolle der Stadt Luzern (sog. Datensouveränität);
- Erarbeitung von Ausstiegs- und Notfallszenarien.

Der grösste Teil dieser Massnahmen ist bereits umgesetzt. Mit den bis anhin umgesetzten Massnahmen darf M365 nur für Daten eingesetzt werden, die **nicht** als «vertraulich» klassifiziert sind. Vertrauliche und geschäftsrelevante Daten müssen weiterhin in den Fachapplikationen und im Geschäftsverwaltungssystem GEVER gespeichert werden.

4. Fazit

Die vom Stadtrat beschlossene IT-Strategie sieht die umfassende Nutzung von Cloud-Services wie M365 ausdrücklich vor. Dieser Entscheid wurde unter sorgfältiger Abwägung der Chancen und Risiken getroffen. Die damit einhergehende Ausweitung der Abhängigkeit von einer einzelnen Anbieterin (Microsoft) ist auch aus Sicht des Stadtrates problematisch, wurde aber bewusst eingegangen, weil die Chancen überwiegen und derzeit keine sinnvollen Alternativen bestehen. Ein Rückzug aus Cloud-Services (sog. «Exit-Strategie») ist folglich nicht Teil der aktuellen strategischen Planung.

Der Stadtrat vertritt die Haltung, dass der Nutzung von Cloud-Services von US-Anbietern wie Microsoft keine datenschutzrechtlichen Bestimmungen entgegenstehen und dass mit den vorgesehenen und grösstenteils umgesetzten vertraglichen, technischen und organisatorischen Massnahmen die Risiken für die Persönlichkeits- und Grundrechte der betroffenen Personen angemessen reduziert werden können.

Der Stadtrat unterstützt die Stärkung der digitalen Souveränität, sieht dies jedoch als primäre Aufgabe auf Bundesebene. Alternativen zur Reduktion der bestehenden Abhängigkeiten werden laufend geprüft. Die Entwicklungen im Bereich der digitalen Souveränität werden aufmerksam verfolgt. Die Stadt tauscht sich diesbezüglich regelmässig mit anderen Deutschschweizer Städten aus und beteiligt sich aktiv in entsprechenden Arbeitsgruppen.

C. Zu den einzelnen Fragen

Zu 1.:
Hat der Stadtrat vom Bericht des DSB und dessen Einschätzungen zur Verwendung von Microsoft M365 Kenntnis genommen? Welchen Handlungsbedarf für die städtische Verwaltung sieht er dadurch?

Sowohl der oben erwähnte Bericht wie auch die im September 2025 publizierte «Datenschutzrechtliche und institutionelle Einschätzung zu M365» wurden vom Stadtrat zur Kenntnis genommen.
Daraus ergaben sich für die Stadt Luzern keine neuen Erkenntnisse. Die Fachstelle DSP und die Projektleitung standen von Beginn weg im Austausch mit dem damaligen und der neuen kantonalen Beauftragten für den Datenschutz (DSB). Die kantonale Datenschutzgesetzgebung wurde als Rahmenbedingung des Vorhabens zur Einführung von M365 von Beginn an miteinbezogen. Die Risiken wurden identifiziert, und geeignete technische und organisatorische Sicherheits- und Datenschutzmassnahmen wurden festgelegt. Für die städtische Verwaltung besteht aus Sicht des Stadtrates der derzeitige Handlungsbedarf darin, die technischen und organisatorischen Sicherheits- und Datenschutzmassnahmen («Basisschutz Cloud+») weiter umzusetzen.

Zu 2.:
Wie geht der Stadtrat allgemein mit Handlungsempfehlungen des DSB um, wenn diese direkt städtische Projekte betreffen? Wie geht der Stadtrat allgemein mit Handlungsempfehlungen des DSB an kantonale oder andere kommunale Behörden um, wenn sich diese auch auf Projekte der Stadt übertragen lassen? Existiert ein Leitfaden für den Umgang mit den Einschätzungen des DSB oder ein Konzept für die proaktive Umsetzung der vom DSB vorgeschlagenen Massnahmen?

Die Publikationen der DSB werden laufend verfolgt, unabhängig davon, ob Projekte der Stadt direkt betroffen sind oder nicht. Die Empfehlungen werden geprüft, mit den bestehenden städtischen Vorgaben («DSP-Standards», siehe oben, Abschnitt Datensicherheit und Risikomanagement) verglichen. Sollten Empfehlungen der DSB darin nicht schon berücksichtigt sein, so wird fallweise geprüft, ob und wie die Vorgaben ergänzt oder angepasst werden. Dadurch ist die proaktive Umsetzung gewährleistet.
Das Verfolgen der aktuellen Entwicklungen sowohl im Bereich des Datenschutzrechts wie auch im Bereich der Informationssicherheit ist ohnehin Teil des Auftrags der Fachstelle DSP.

Zu 3.:
Welche Datenklassifikationen verwendet die Stadt Luzern für die digitale Bearbeitung von Daten, insbesondere in der Cloud von Microsoft? Inwiefern sieht der Stadtrat Handlungsbedarf in Bezug auf die Einschätzung des DSB, wonach die Triagierung der Daten für die Bearbeitung mit M365 bis zur Stufe «vertraulich» nicht datenschutzkonform sei?

Die Datenklassifikation ist nicht abhängig von der Art der Bearbeitung (digital/Papier), sondern richtet sich nach den rechtlichen Bestimmungen einerseits und den potenziellen Folgen einer unrechtmässigen Offenlegung andererseits. Die Stadt Luzern verwendet die Klassifizierung «Vertraulich» für Schriftgut, dessen Geheimhaltung durch besondere Vorschriften geregelt ist oder dessen unrechtmässiges oder frühzeitiges Bekanntwerden zu einem schwerwiegenden Schaden für natürliche oder juristische Personen, die Öffentlichkeit, die Behörden oder die Verwaltung führen kann (Art. 37a Organisationsverordnung vom 28. August 2002; sRSL 0.5.1.1.2). Darunter fällt gemäss Art. 37a Organisationsverordnung auch Schriftgut mit besonders schützenswerten Personendaten.
Als Schriftgut gelten alle Dokumente und Datensätze unabhängig vom Informationsträger (Art. 36 Organisationsverordnung).

Für Daten, die «Vertraulich» klassifiziert sind, bestehen strengere Bearbeitungsregeln, insbesondere hinsichtlich der Zugangskontrolle und der Datenspeicherorte. Diese Regeln gelten allgemein und nicht nur begrenzt auf Cloud-Services von Microsoft.
Gestützt auf die Prüfung der rechtlichen Rahmenbedingungen erachtet der Stadtrat die Bearbeitung von Daten mit M365 bis zur Stufe «Vertraulich» grundsätzlich als rechtmässig und im Rahmen der Datenschutzgesetzgebung als zulässig. Voraussetzung für die Bearbeitung von als «Vertraulich» klassifizierten Daten in der städtischen M365-Umgebung ist, dass das Schutzniveau «Basisschutz Cloud+» nachweislich erreicht und aufrechterhalten wird. Durch das Schutzniveau wird sichergestellt, dass keine hohen Risiken bestehen und das Grundrecht auf informationelle Selbstbestimmung gemäss Art. 13 BV gewährleistet bleibt.

Zu 4.:
Wie wird sichergestellt, dass alle Mitarbeitenden die Vorgaben zur Datenklassifikation korrekt einhalten?

Auf der internen Lernplattform steht sämtlichen Mitarbeitenden eine Schulung zur Klassifizierung von Unterlagen zur Verfügung. Zusätzlich bestehen Merkblätter sowie Hilfestellungen mit Anwendungsbeispielen, um das Thema zu erklären. Bei Unsicherheiten können sich Mitarbeitende an die Registratorin oder den Registrator innerhalb ihrer Organisationseinheit wenden. Diese unterstützen die Mitarbeitenden auch bei Fragen zur Klassifikation.

Zu 5.:
Ist es ausgeschlossen, dass US-amerikanische Behörden Zugriff auf die Daten oder Kontrolle über die Dienste in der Microsoft-Cloud erhalten? Falls dies nicht ausgeschlossen ist: Was ist die Haltung des Stadtrates zu diesem Risiko?

Das Risiko, dass Behörden bei Microsoft die Herausgabe von Daten der Stadt Luzern erzwingen könnten, kann nicht vollständig ausgeschlossen werden.
Im Zusammenhang mit den USA werden vor allem der US CLOUD Act (Clarifying Lawful Overseas Use of Data Act) sowie FISA (Foreign Intelligence Surveillance Act) erwähnt. Der US CLOUD Act ermöglicht US-Strafverfolgungsbehörden, bei schweren Straftaten die Herausgabe von Daten zu verlangen. FISA ermöglicht gewissen US-Behörden (insbesondere FBI und CIA), Daten über bestimmte Zielpersonen zu verlangen. Diese Gesetze gelten für alle Unternehmen mit Sitz in den USA oder anderen rechtlichen Beziehungen zu den USA (z. B. eine Zweigniederlassung). Diese Gesetze begründen in spezifischen Fällen einen Anspruch auf Herausgabe von Daten. Es findet kein direkter Zugriff der Behörden auf die Daten statt.
Es wurden Massnahmen ergriffen, damit das Risiko einer Herausgabe von Daten an US-amerikanische Behörden minimiert wird. Zu diesen Massnahmen zählt insbesondere die EU Data Boundary. Mit dieser wird sichergestellt, dass die Daten nur innerhalb der EU/EFTA bearbeitet werden. Die Datenspeicherung erfolgt grundsätzlich nur in Schweizer Rechenzentren. Zudem wird mit vertraglichen Vereinbarungen der Schutz der Daten vor der Herausgabe an Behörden ergänzt. Microsoft ist verpflichtet, Herausgabebegehren von Behörden ausserhalb der EU/EFTA nur gemäss Schweizer Recht zu bearbeiten. Die Wirksamkeit dieser Massnahmen wird überwacht, um sicherzustellen, dass das Risiko auf tiefem Niveau verbleibt.
Zu beachten ist auch, dass nach Ansicht des Bundesrates Institutionen in den USA ein angemessenes Datenschutzniveau gewährleisten können. Im Rahmen des Swiss-U.S. Data Privacy Frameworks ist es zulässig, Personendaten aus der Schweiz an zertifizierte Institutionen in den USA zu übermitteln, ohne zusätzliche Garantien. Die zertifizierten Institutionen gewährleisten ein angemessenes Schutzniveau für Personendaten. Microsoft ist zertifiziert gemäss dem Swiss-U.S. Data Privacy Framework.

Es kann auch nicht ausgeschlossen werden, dass eine Behörde Microsoft dazu zwingen könnte, ihre Cloud-Dienste für bestimmte Kunden zu sperren. Dies stellt jedoch kein Microsoft- oder US-spezifisches Risiko dar, sondern kann prinzipiell auch bei jedem anderen Dienstleister, von dem die Stadt abhängig ist, eintreten.

Wie die Stadt auf eine plötzliche Nichtverfügbarkeit eines solchen Dienstes reagieren würde, ist in den einleitenden Bemerkungen im Abschnitt 1 Digitale Souveränität und Vendor Lock-in beschrieben.

Zu 6.:
Gemäss DSB bedarf es eines kontinuierlichen Risikomanagements im Zusammenhang mit der Nutzung von Microsoft M365. Gibt es ein solches Risikomanagement bei der Stadt Luzern? Wenn Ja, wie ist es ausgestaltet?

In der Stadt Luzern besteht ein integrales, kontinuierliches Risikomanagement, das neben dem Business Continuity Management insbesondere auch operationelle Risiken beinhaltet. Datenschutz- und Informationssicherheitsrisiken sind dabei als operationelle Risiken miteingeschlossen.
Für das Management von Datenschutz- und Informationssicherheitsrisiken auf Ebene einzelner Projekte und Vorhaben (wie z. B. die Einführung von M365) ist die Fachstelle DSP zuständig. Die Ausgestaltung dieses Risikomanagements ist in den einleitenden Bemerkungen im Abschnitt 3 Datensicherheit und Risikomanagement beschrieben. Mit dieser Systematik und der Abstützung auf etablierte Normen ist sichergestellt, dass keine wesentlichen Risiken übersehen und keine wichtigen Massnahmen zur Risikoreduktion ausser Acht gelassen werden.

Zu 7.:
Verfügt die Stadt Luzern über eine Exit-Strategie zu M365, wie sie vom DSB empfohlen wird? Wenn Ja, wie sieht diese konkret aus?

Die aktuelle IT-Strategie der Stadt Luzern sieht keinen Rückzug aus M365 oder anderen Cloud-Services vor. Eine sogenannte «Exit-Strategie» besteht demzufolge nicht.

Hingegen erfordert der «Basisschutz Cloud+» auch für M365 die Erarbeitung von Ausstiegsszenarien. Was dies beinhaltet, ist in den einleitenden Bemerkungen im Abschnitt 1 näher erläutert. Für die städtische M365-Umgebung ist diese Massnahme zum Zeitpunkt der Beantwortung dieser Interpellation noch nicht umgesetzt, aber geplant.

Zu 8.:
Wie schätzt der Stadtrat die Risiken der Abhängigkeit von amerikanischen und chinesischen IT-Anbietern generell ein? Wie beurteilt der Stadtrat das vom DSB beschriebene Risiko eines Vendor Lock-in im Zusammenhang mit M365? Welchen Stellenwert geniesst die digitale Souveränität für die Stadt Luzern, und welche konkreten Massnahmen werden getroffen, um diese nachhaltig sicherzustellen?

Auf staatlicher Ebene ist die digitale Souveränität in erster Linie Aufgabe des Bundes. Es kann nicht Aufgabe einer Gemeinde sein, staatliche digitale Infrastruktur aufzubauen. Es ist indessen Aufgabe der Stadt, wie es Aufgabe jeder Verwaltungseinheit ist, die Kontrolle über die Daten zu gewährleisten und sich der einzelnen Aspekte der Ausstiegszenarien bewusst zu sein.

Die Abhängigkeit von asiatischen und amerikanischen IT-Anbietern ist bei der Stadt Luzern – wie bei den meisten Verwaltungen und Unternehmen der Privatwirtschaft – sehr hoch. Sie betrifft sowohl die Hersteller von Hardware für Infrastruktur und Netzwerke wie auch Endgeräte wie Notebooks und Smartphones, Software für betriebsrelevante Rechenzentrumsanwendungen, Betriebssysteme, Bürosoftware und Cloud-Dienste. Diese Abhängigkeit ist zum Teil eine Folge der freien Marktwirtschaft, da der globale Wettbewerb in diesen Regionen zu einer Konzentration von Innovation und Produktion geführt hat. Gleichzeitig resultiert sie aus politischen Versäumnissen und strukturellen Schwächen Europas in der Technologie- und Industriepolitik. Geringere Risikobereitschaft und fehlende einheitliche Digitalpolitik haben dazu geführt, dass Europa in diesem Bereich weniger konkurrenzfähig ist.

Das Risiko der Abhängigkeit, insbesondere von Microsoft, ist bekannt, als Toprisiko bewertet und wird vom Stadtrat getragen. Die Behandlung des Risikos erfolgt im Rahmen des städtischen Risikomanagements. Der Stadtrat wird periodisch darüber informiert, nimmt die Risiken sowie die geplanten Massnahmen zu deren Begrenzung und Reduktion zur Kenntnis und ordnet bei Bedarf weitere Massnahmen an.

Das vom DSB beschriebene Risiko eines so genannten Vendor Lock-in stellt kein Datenschutzrisiko im eigentlichen Sinne dar. Das Risiko besteht darin, dass ein Wechsel zu einem anderen Anbieter nur mit erheblichen Nachteilen und hohem finanziellem und operativem Aufwand möglich ist. Dieses Risiko besteht auch mit anderen (schweizerischen) Software- und IT-Lieferanten, die Fachapplikationen für Verwaltungen anbieten, und nicht nur im Zusammenhang mit M365.
Bei M365 werden die Chancen und Risiken eines breiten Einsatzes von Microsoft-Produkten sorgfältig gegeneinander abgewogen. Den Risiken stehen massgebliche Chancen gegenüber:
- Die hohe Kompatibilität und Interoperabilität zwischen den verschiedenen Microsoft-Produkten und -Services führen im Betrieb zu erheblichen Erleichterungen und Einsparungen.
- Die umfassende Unterstützung und Dokumentation durch Microsoft sowie die sehr grosse Anzahl Partnerfirmen in der Schweiz führen zu einfacherer Integration und intelligenten Lösungen.
- Die granularen Konfigurationseinstellungen ermöglichen eine durchgängige und wirksame Umsetzung von Sicherheits- und Datenschutzvorgaben.
- Eine grosse Benutzerbasis und eine aktive Community, die Erfahrungen und Wissen teilt, tragen bei Problemstellungen zur schnelleren Lösung bei.
- Auf dem Arbeitsmarkt ist eine sehr grosse Anzahl an Spezialisten verfügbar, um die Lösungen zu entwickeln und zu betreiben.

Die Stadt Luzern tauscht sich seit Jahren regelmässig mit den grossen Deutschschweizer Städten Basel, Bern, Biel, Chur, Thun, St. Gallen, Winterthur und Zürich zu Informatik-Themen aus (City-Network). Der Austausch findet sowohl auf der obersten Führungsebene wie auch auf der technischen Ebene statt. Innerhalb des City-Networks ist eine Arbeitsgruppe im Aufbau, die sich mit Alternativen zu M365-Produkten befassen wird. Die Stadt Luzern wird Mitglied dieser Arbeitsgruppe sein.

Die Digitale Verwaltung Schweiz (DVS) lanciert eine neue Arbeitsgruppe Cloud-Infrastrukturen. Die Arbeitsgruppe wird in Co-Leitung von der Geschäftsstelle DVS und dem Programm «Arbeitsgruppe Swiss Government Cloud (SGC)» geführt. Sie bietet Verantwortlichen für Cloud-Infrastrukturen der öffentlichen Verwaltungen von Städten, Gemeinden, Kantonen und dem Bund einen strukturierten Rahmen für einen regelmässigen Wissens- und Informationsaustausch. Die Arbeitsgruppe soll dazu beitragen, dass Städte, Gemeinden, Kantone und der Bund die Herausforderungen der Cloud-Technologie in der Anwendung im Verwaltungskontext gemeinsam angehen können. Der ICT- und Security-Architekt der Stadt Luzern wird ein Mitglied der neuen Arbeitsgruppe werden.

Unabhängig davon wird die Stadt Luzern für ihre M365-Umgebung die Datensouveränität sicherstellen und Ausstiegsszenarien erarbeiten. Siehe dazu die einleitenden Bemerkungen, Abschnitt 1.