KANTON
LUZERN

Kantonale Datenschutzbeauftragte
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 61 00
datenschutz@lu.ch
www.datenschutz.lu.ch

A-Post
Stadt Luzern
Fachstelle digitale Sicherheit und Privatsphäre
Hirschengraben 17
6002 Luzern

Luzern, 22. Juli 2025 spd

Stellungnahme DSB zum Vorhaben Azzurro 2.0 der Stadt Luzern (Einführung M365)

Sehr geehrte Damen und Herren

Die Datenschutzbeauftragte (DSB) bedankt sich bei der Stadt Luzern für die Einreichung der folgenden Unterlagen:

- Schreiben Vorabkonsultation - Programm Azzurro 2.0
- Datenschutz-Folgenabschätzung (DSFA)
- Liste mit Massnahmen (Excel)

Wir entschuldigen uns für die Verzögerung und nehmen zum vorliegenden Vorhaben wie folgt Stellung:

1 Einleitung

Die Stadt Luzern hat den kantonalen Datenschutzbeauftragten (DSB) frühzeitig über das Programm Azzurro 2.0 informiert und sich im Rahmen mehrerer Konsultationen und Arbeitstreffen proaktiv mit den datenschutzrechtlichen Fragestellungen auseinandergesetzt. Bereits in einer frühen Phase des Projekts wurden die Empfehlungen des Datenschutzbeauftragten aus der Risikoanalyse von 2021 aufgegriffen und in die Weiterentwicklung des Programms integriert.

Die nun vorliegenden Unterlagen – bestehend aus dem Schreiben zur Vorabkonsultation, der umfassenden Datenschutz-Folgenabschätzung (DSFA) sowie der detaillierten Massnahmenliste – sind von hoher Qualität und zeichnen sich durch eine sorgfältige Analyse der rechtlichen und technischen Rahmenbedingungen aus. Besonders hervorzuheben ist die konsequente Ausrichtung des Sicherheitsniveaus an internationalen Standards (ISO/IEC 27002 und 27701) sowie die Festlegung eines spezifischen Schutzkonzepts («Basisschutz Cloud +»), das über die gesetzlichen Mindestanforderungen hinausgeht. Die systematische Berücksichtigung

von Restrisiken und die Planung von Exit-Strategien unterstreichen die strategische Weitsicht des Programms.

Diese Vorabkonsultation zeigt, dass die Stadt Luzern den Datenschutz und die Datensicherheit als integrale Bestandteile der Digitalisierung versteht und bereit ist, angemessene organisatorische und technische Massnahmen umzusetzen, um die Rechte der betroffenen Personen zu wahren.

Gleichzeitig ist festzuhalten, dass der damalige Datenschutzbeauftragte mehrfach, letztmals im Juli 2024 nach einer vertieften Analyse der geplanten Einführung von M365 in einer Aktennotiz auf wesentliche rechtliche und strategische Risiken hingewiesen hat. Diese Bedenken betreffen insbesondere die Bearbeitung von sensitiven Personendaten[1] mit M365, die digitale Souveränität, den Schutz der Grundrechte nach Art. 13 Abs. 2 BV sowie die Abhängigkeit von einem einzelnen Anbieter. Vor diesem Hintergrund knüpfen die nachfolgenden Feststellungen und Empfehlungen an die bisherige Begleitung des Projekts an.

2 Bearbeitung von sensitiven Personendaten mit M365

Die DSFA hält fest, dass die rechtlichen Rahmenbedingungen eine Bearbeitung von klassifizierten bzw. vertraulichen Daten in einer Cloud-Lösung zulassen, insbesondere besonders schützenswerte Personendaten sowie Daten, die dem Amtsgeheimnis oder einem besonderen Amtsgeheimnis unterliegen. Daten, die einer Geheimnispflicht unterliegen, die eine Bearbeitung durch Hilfspersonen nicht zulässt, gäbe es gemäss aktueller Kenntnis innerhalb der Stadt Luzern nicht.

2.1 Stellungnahme und Empfehlung für die Bearbeitung von sensitiven Personendaten mit M365

Jede Datenbekanntgabe durch ein öffentliches Organ bedarf einer hinreichenden gesetzlichen Grundlage. Für die Bekanntgabe von Daten an ausländische Strafverfolgungsbehörden gilt – soweit keine andere staatsvertragliche Regelung besteht –das Rechtshilfegesetz des Bundes[2].

Der US-Amerikanische CLOUD Act[3] erlaubt es den dortigen Strafverfolgungsbehörden, die dem Act unterstehenden Cloud-Anbieter zur Herausgabe von Daten zu verpflichten, auch wenn die Daten in der Schweiz oder der EU gespeichert sind. Betrifft dies Personendaten, die der Anbieter im Auftrag eines öffentlichen Organs bearbeitet, würde eine Bekanntgabe unter Umgehung des Rechtshilfewegs ohne in der Schweiz anerkannte Rechtsgrundlage erfolgen und somit unzulässig sein.[4]

Nach der auf das öffentliche Recht spezialisierten Lehre spielt es mindestens bei besonders schützenswerten Personendaten keine Rolle, wie wahrscheinlich ein Zugriff der US-Behörden auf Daten unter der Verantwortung eines öffentlichen Organs ist: Einerseits wird die Tatsache, dass der Cloud-Anbieter gesetzlich dazu verpflichtet werden kann, die Daten anders zu bear-

[1] In diesem Dokument dient der Begriff «sensitive Personendaten» als Oberbegriff für alle Personendaten mit einem erhöhten Schutzbedarf, d.h. besonders schützenwerte Personendaten, Persönlichkeitsprofile und Personendaten unter einer gesetzlichen Geheimhaltungspflicht.
[2] Bundesgesetz vom 20.03.1981 über internationale Rechtshilfe in Strafsachen (IRSG; SR 351.1).
[3] Clarifying Lawful Overseas Use of Data (CLOUD) Act.
[4] MARKUS SCHEFER/PHILIP GLASS, Der grundrechtskonforme Einsatz von M365 durch öffentliche Organe in der Schweiz – Eine Analyse am Beispiel des Kantons Zürich, Editions Weblaw, Bern 2023, Ziff. 6.3.4.2.1 (S. 35 f.); ASTRID EPINEY/NULA FREI, Verfassungs- und völkerrechtliche Vorgaben der Bekanntgabe von Personendaten ins Ausland im Rahmen einer Auftragsbearbeitung, Rechtsgutachten im Auftrag des Rechtsamtes der Direktion für Inneres und Justiz des Kantons Bern, Oktober 2023, N. 93 f. (S. 37).

beiten, als das öffentliche Organ es dürfte, generell als Rechtsfrage angesehen, die keiner Risikoanalyse zugänglich ist.[5] Andererseits werden die allgemeinen Vorschriften zur Auftragsbearbeitung in den Datenschutzgesetzen nicht als ausreichend erachtet, um besonders schützenswerte Personendaten in die Cloud eines US-Unternehmens auszulagern und den Eingriff in die Rechte der betroffenen Personen durch Schaffung eines Risikos der Bekanntgabe an US-Behörden zu legitimieren.[6]

Bei der Auslagerung von Personendaten, die einem Geheimnisschutz unterliegen, geht die Lehre davon aus, dass eine gesetzlich vorgesehene Zugriffsmöglichkeit – wie jene nach dem CLOUD Act – eine Verletzung der Geheimhaltungspflicht darstellt, die keinen Raum für eine Risikoabwägung lässt.[7]

Schliesslich ist zu beachten, dass die jüngeren politischen Veränderungen in den USA die rechtsstaatlichen Garantien des amerikanischen Rechts insgesamt stark relativieren und nebst dem Schutz der Vertraulichkeit von sensitiven Personendaten auch die Verfügbarkeit der Daten in Cloud-Services von US-Anbieter weniger gewährleistet ist.
Werden im Rahmen einer Auslagerung Personendaten in die USA übermittelt, so sind die Empfehlungen nach der betreffenden Publikation von privatim zu beachten.[8]

Aus heutiger Sicht ist der Einsatz von M365 zur Bearbeitung von sensitiven Personendaten nicht zulässig. Es fehlt an einer hinreichend bestimmten gesetzlichen Grundlage, wie sie für schwerwiegende Eingriffe in die informationelle Selbstbestimmung nach Art. 36 Abs. 1 BV zwingend erforderlich ist. Die geltenden Bestimmungen des kantonalen Datenschutzgesetzes (KDSG) und seiner Verordnung (KDSV) reichen nicht aus, um die Bearbeitung solcher Daten in einer transnational regulierten Cloud-Infrastruktur zu legitimieren. Darüber hinaus verliert die öffentliche Verwaltung mit dem Einsatz von M365 in relevanten Teilen die Kontrolle über die Datenbearbeitung, was mit den datenschutzrechtlichen Anforderungen an Weisungsgebundenheit, Transparenz und effektive Kontrollmöglichkeiten nicht vereinbar ist.

Die Bearbeitung von sensitiven Personendaten (besonders schützenswerte Personendaten und Daten, die einer gesetzlichen Geheimhaltungspflicht unterliegen) durch Microsoft Cloud-Services (ohne weitere technische Massnahmen[9]), kann nicht einer Risikobeurteilung zugeführt werden.

Die DSB erachtet die Nutzung von M365 zur Bearbeitung von besonders schützenswerten Personendaten und Daten unter einem gesetzlichen Geheimnisschutz durch die Stadt Luzern als unzulässig, sofern die Daten nicht vom verantwortlichen Organ selbst verschlüsselt werden und Microsoft keinen Zugang zum Schlüssel hat.

2.2 Empfehlung

Die Datenschutzbeauftragte empfiehlt der Stadt Luzern, besonders schützenswerte Personendaten sowie Daten, die einer gesetzlichen Geheimhaltungspflicht unterliegen, konsequent zu klassifizieren und deren Bearbeitung mit M365 zu unterlassen. Solange keine hinreichend be-

[5] EPINEY/FREI (Fn. 4), N. 3 (S. 1) und 95 (S. 37 f.).
[6] SCHEFER/GLASS (Fn. 4), Ziff. 6.3.4.3 (S. 41) und 7.1.11 (S. 57).
[7] EPINEY/FREI (Fn. 4), N. 101 (S. 40).
[8] Publikation «Übermittlung von Personendaten an Organisationen in den USA auf der Grundlage des Swiss-US Data Privacy Framework» vom 08.07.2025
[9] Verschlüsselung der Daten in allen drei Zuständen und nur das Organ hat Zugriff auf den Schlüssel.

stimmte gesetzliche Grundlage für die Auslagerung dieser Daten in eine transnational regulierte Cloud-Infrastruktur eines US-Anbieters besteht und keine technischen Massnahmen implementiert sind, die einen Zugriff des Anbieters selbst (inklusive Schlüsselzugang) zuverlässig ausschliessen, ist der Einsatz von M365 für sensitive Personendaten unzulässig.

Es wird der Stadt Luzern ferner empfohlen, alternative Szenarien zu prüfen, die eine Bearbeitung sensitiver Personendaten innerhalb der eigenen Infrastruktur (On-Premises) oder mit Lösungen ermöglichen, die keinen extraterritorialen Rechtszugriff unterliegen. Dabei sind sowohl hybride Ansätze als auch Verschlüsselungslösungen zu evaluieren, bei denen der Schlüssel ausschliesslich in der Hoheit des verantwortlichen Organs verbleibt.

3 Zur verfassungsrechtlichen Beurteilung des Einsatzes von M365

In den eingereichten Unterlagen wird ausgeführt, die verfassungsmässigen Garantien könnten auch beim Einsatz von Microsoft 365 (M365) gewahrt werden. Diese Einschätzung steht im deutlichen Spannungsverhältnis zu den Ergebnissen des Gutachtens von Prof. Dr. Markus Schefer und Dr. Philip Glass vom 6. Juli 2023 betreffend den grundrechtskonformen Einsatz von M365 durch Gemeinden im Kanton Zürich.

Das Gutachten analysiert eingehend die verfassungsrechtliche Lage unter Berücksichtigung von Art. 13 Abs. 2 BV sowie der kantonalen Datenschutzgesetzgebung. Es gelangt zu dem Ergebnis, dass der Einsatz von M365 eine Vielzahl von Grundrechtseingriffen begründet, deren Rechtfertigung derzeit weder durch die gesetzliche Grundlage noch durch die umgesetzten technischen und organisatorischen Massnahmen gewährleistet ist:

1. Übertragung der Datenherrschaft und Kontrollverluste (S. 27–29)
Schefer/Glass stellen fest, dass die Auslagerung der Datenverarbeitung an einen Anbieter wie Microsoft zu einem faktischen Kontrollverlust der datenverarbeitenden öffentlichen Stelle führt. Dies betrifft sowohl den tatsächlichen Zugriff auf die Daten als auch die rechtliche Situation, da US-amerikanische Behörden im Rahmen des CLOUD Act und Stored Communications Act (SCA) potentiell Zugriff auf Daten erhalten können, auch wenn diese in der Schweiz oder der EU gespeichert werden. Dieser Kontrollverlust wirkt sich unmittelbar auf die Betroffenen aus und wird als schwerwiegender Eingriff in die informationelle Selbstbestimmung qualifiziert.

2. Fehlende hinreichende gesetzliche Grundlage (S. 35–37)
Das Gutachten betont, dass für einen schweren Grundrechtseingriff eine klare und detaillierte gesetzliche Grundlage erforderlich ist (Art. 36 Abs. 1 BV). Die kantonalen Datenschutzgesetze und allgemeinen Rechtsgrundlagen reichen nach Einschätzung der Autoren nicht aus, um die mit dem Einsatz von M365 verbundenen strukturellen Risiken zu legitimieren. Insbesondere fehle es an einer Regelung, die die spezifischen Risiken von Cloud-Diensten mit extraterritorialer Wirkung adressiert.

3. Verhältnismässigkeit und Zumutbarkeit des Restrisikos (S. 39–43)
Trotz umfangreicher Sicherungsmassnahmen verbleibt nach Auffassung von Schefer/Glass ein Restrisiko, das aus verfassungsrechtlicher Sicht nicht als zumutbar angesehen werden kann. Dies gilt insbesondere im Hinblick auf die Abhängigkeit von einem einzelnen Anbieter (Vendor Lock-in) sowie den fehlenden effektiven Rechtsschutz der Betroffenen gegenüber Zugriffen durch Dritte.

3.1 Bewertung des Azzurro-Ansatzes

Die Stadt Luzern hat mit dem «Basisschutz Cloud +»-Konzept und den ergänzenden Massnahmen zweifellos substantielle Anstrengungen unternommen, um datenschutzrechtliche Risiken zu mitigieren. Positiv hervorzuheben sind insbesondere:

- die Ausrichtung auf ISO/IEC 27002 und 27701 Standards,
- die geplanten Exit-Strategien zur Reduktion der Anbieterabhängigkeit,
- die Durchführung einer umfassenden Datenschutz-Folgenabschätzung mit Risikoanalyse.

Gleichwohl ist festzustellen, dass diese Massnahmen das von Schefer/Glass identifizierte strukturelle Problem der Übertragung der Datenherrschaft an einen US-Anbieter nicht auflösen. Auch aus Sicht des kantonalen Datenschutzrechts kann nicht ausgeschlossen werden, dass ein Einsatz von M365 ohne spezifische gesetzliche Grundlage und flankierende Rechtsinstrumente verfassungsrechtlich problematisch bleibt.
Vor diesem Hintergrund erscheint es angezeigt, die Aussage, M365 sei mit den verfassungsmässigen Garantien vereinbar, zurückhaltend zu bewerten. Es sollte geprüft werden, ob mildere Mittel (Art. 36 Abs. 3 BV) zur Verfügung stehen, die eine gleichwertige Funktionalität ohne vergleichbare Eingriffsintensität ermöglichen.

In ihrem Schreiben führt die Stadt Luzern aus, ein Weiterbetrieb von Exchange und Skype „On-Premises" sei in absehbarer Zukunft nicht mehr garantiert, und Microsoft sei als Dienstleisterin im Bereich der Büroautomation marktführend, wobei deren Services unverzichtbare Vorteile gegenüber anderen Lösungen böten. Diese Einschätzung erweist sich jedoch als verkürzt: Exchange ist weiterhin als Subscription Edition (Exchange Server SE) verfügbar und wird von Microsoft mit erweitertem Support angeboten. Gleiches gilt für Skype for Business Server, dessen Lifecycle ebenfalls eine On-Premises-Nutzung weiterhin ermöglicht. Die pauschale Annahme, ein Verbleib auf On-Premises-Lösungen sei ausgeschlossen, ist daher faktisch nicht korrekt.

Darüber hinaus ist die Argumentation der „Alternativlosigkeit" aus datenschutzrechtlicher Sicht heikel. Der Einsatz von M365 verstärkt die bestehende Abhängigkeit von einem einzelnen Anbieter (Vendor Lock-in), insbesondere da mit der Integration von Teams auch Kollaboration und Telefonie künftig vollständig über die Microsoft-Cloud abgewickelt werden sollen. Nach Art. 36 Abs. 3 BV ist im Rahmen der Verhältnismässigkeit stets zu prüfen, ob mildere Mittel existieren, die den gleichen funktionalen Bedarf mit geringerer Eingriffsintensität decken. Solche Alternativen – etwa der Betrieb von Exchange und Skype On-Premises, hybride Szenarien oder der Einsatz datenschutzfreundlicherer Kollaborationsplattformen – wurden in den Unterlagen nur am Rande geprüft und nicht in die Risikoabwägung einbezogen.

3.2 Empfehlung

Die DSB empfiehlt, die Prüfung möglicher Alternativen vertieft nachzuholen und dabei insbesondere Optionen einzubeziehen, die eine Reduktion der Anbieterabhängigkeit erlauben. Zudem sollte die Argumentation der Alternativlosigkeit vermieden werden, da sie dem verfassungsrechtlichen Erfordernis einer sorgfältigen Abwägung aller in Betracht kommenden Massnahmen zuwiderläuft. Bis zum Vorliegen einer solchen Analyse ist von einer Ausweitung der Nutzung von M365 – insbesondere auf sensitive Anwendungsbereiche – abzusehen.

4 Schlussbemerkung

Das Programm Azzurro 2.0 der Stadt Luzern zeigt, dass Digitalisierungsvorhaben im öffentlichen Sektor zunehmend mit komplexen datenschutzrechtlichen Fragestellungen verbunden sind. Die Stadt hat mit der frühzeitigen Einbindung des kantonalen Datenschutzbeauftragten einen wichtigen Beitrag zur Verankerung des Datenschutzes im Projekt geleistet und substantielle Massnahmen zur Risikoabschwächung ergriffen.

Gleichwohl erfordert der geplante Einsatz von M365 eine differenzierte Bewertung. Die Feststellungen in dieser Stellungnahme verdeutlichen, dass insbesondere die Bearbeitung sensitiver Personendaten in einer Cloud-Infrastruktur eines US-Anbieters nicht primär eine Frage der Risikoabwägung ist. Vielmehr setzen die verfassungsrechtlichen und datenschutzrechtlichen Vorgaben klare Schranken: Ein potenzieller Zugriff durch US-Behörden unter dem CLOUD Act stellt unabhängig von seiner Eintrittswahrscheinlichkeit eine rechtliche Problematik dar. Die blosse Möglichkeit, dass der Anbieter gesetzlich verpflichtet werden könnte, Daten anders zu bearbeiten, als es dem öffentlichen Organ erlaubt wäre, genügt, um den Einsatz für sensitive Personendaten als unzulässig zu qualifizieren.

Die Schranken bei der Übertragung der Datenherrschaft in IT-Systeme mit extraterritorialen Rechtszugriffen und das Risiko der zunehmenden Anbieterabhängigkeit sind von struktureller Natur und lassen sich auch durch umfangreiche organisatorische und technische Massnahmen nicht vollständig ausräumen.

Es ist hervorzuheben, dass diese Einschätzung nicht isoliert steht. Sie entspricht der einheitlichen Haltung der kantonalen Datenschutzaufsichtsbehörden in der Schweiz, wie sie in der Konferenz der schweizerischen Datenschutzbeauftragten (privatim) regelmässig ausgetauscht und konsolidiert wird. Die von privatim erarbeiteten Empfehlungen und Stellungnahmen dienen öffentlichen Organen als Orientierungshilfe und spiegeln einen breiten Konsens der Aufsichtsbehörden wider. Dieser Konsens hat zwar keine unmittelbare rechtliche Bindungswirkung, dokumentiert jedoch die kohärente datenschutzrechtliche Bewertung auf Aufsichtsbehördenebene. Für Gemeinwesen bietet er eine wichtige Grundlage für die eigene Risiko- und Rechtslagebeurteilung im Bereich Cloud-Services und digitale Souveränität.

Vor diesem Hintergrund wird die Stadt Luzern erneut dazu angehalten, die im Rahmen dieser Stellungnahme formulierten Empfehlungen eingehend zu prüfen und die Umsetzung des Programms so zu gestalten, dass die Grundrechte der betroffenen Personen nachhaltig gewahrt bleiben.

Im Übrigen verweist die DSB auf die detaillierten Erläuterungen über die datenschutzrechtliche und institutionelle Einschätzung zu M365, welcher dieser Empfehlung beiliegen. Zudem legen wir diesem Schreiben das Merkblatt «Besonders schützenswerte Personendaten» bei.

5 Hinweis zur Veröffentlichung

Die Datenschutzbeauftragte behält sich vor, die vorliegende Stellungnahme auf der Website öffentlich zugänglich zu machen. Dies steht im Einklang mit dem seit 1. Juni 2025 geltenden Öffentlichkeitsprinzip, wonach amtliche Informationen der Verwaltung grundsätzlich zugänglich sind, sofern keine überwiegenden öffentlichen oder schützenswerten privaten Interessen einer Veröffentlichung entgegenstehen.

Angesichts der hohen öffentlichen und politischen Relevanz des geplanten Einsatzes von M365 erscheint eine transparente Publikation der Stellungnahme im besonderen öffentlichen Interesse. Sie dient der Förderung eines informierten politischen Diskurses zu Fragen der digitalen Souveränität, des Datenschutzes und der Abhängigkeit von globalen Cloud-Diensten.

Sofern die Stadt Luzern keine überwiegenden öffentlichen oder schützenswerten privaten Interessen geltend macht, kann die Stellungnahme nach Ablauf einer Frist von 30 Tagen ab Zustellung veröffentlicht werden.

Freundliche Grüsse

Datenschutzbeauftragte des Kantons Luzern

(Brief ohne Unterschrift)