KANTON
LUZERN

Kantonaler Datenschutzbeauftragter
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 61 00
datenschutz@lu.ch
www.datenschutz.lu.ch

Kanton Luzern
Dienststelle Informatik

Luzern, 18. Juni 2024

Stellungnahme des Datenschutzbeauftragten zur geplanten Einführung von M365 in der kantonalen Verwaltung

Sehr geehrter Herr Raeber, lieber Andreas
Sehr geehrte Damen und Herren

Der Datenschutzbeauftragte (DSB) nimmt zur geplanten Einführung von M365 in der kantonalen Verwaltung wie folgt Stellung.

1 Ausgangslage

Der Kanton Luzern plant die Einführung von M365 Cloud-Services von Microsoft. Im Rahmen der Initialisierung des Vorhabens hat die DIIN im Sinne einer Vorstudie eine abstrakte Datenschutz-Folgenabschätzung (DSFA) mit externer Unterstützung durchgeführt. Der DSB hat diese DSFA intensiv begleitet. Gegenstand der DSFA und damit der zugrundeliegenden Risikobetrachtung sind folgende M365 Cloud-Services von Microsoft:

- Microsoft OneDrive for Business und Microsoft SharePoint Online
- Microsoft Office 365 (Word, Excel, Access, PowerPoint, etc.)
- Microsoft Teams
- Microsoft Entra ID (ehemals Azure Active Directory)
- Microsoft Defender Suite

Nicht Gegenstand der DSFA sind:

- Arbeitsplätze und Mobiltelefone (PC, Laptops, etc.) der Mitarbeitenden des Kantons, inkl. der darauf installierten Betriebssysteme und Software
- Netzwerkkonfiguration des Kantons zur Anbindung an M365 und der Mitarbeitenden im Homeoffice
- Anbindungen von Microsoft Teams an das Telefonnetz (PSTN)
- Active Directory (und weitere Identity Provider), betrieben innerhalb der Infrastruktur des Kantons
- E-Mail-Server, betrieben innerhalb der Infrastruktur des Kantons
- Microsoft Exchange Online

- Alle weiteren Microsoft Office 365 Apps und Services (wie beispielsweise Microsoft Streams und Sway)

Betrachtet hat das Vorhaben den aktuellen Stand von M365 Cloud-Services von Microsoft, d.h. einerseits gestützt auf bekannte Vertragsgrundlagen per 2024[1] und andererseits ohne bevorstehende Integration neuer Funktionen (wie Copilot) oder Erneuerung grundlegender Infrastrukturkomponenten (Microsoft Entra ID, Microsoft Entra Connect Sync). Das Vorhaben hat einen Risikobericht als zusammenfassende Essenz der DSFA erstellt. **Der DSB hält fest, dass der Bericht an den Regierungsrat über die Restrisiken des Einsatzes von Microsoft M365 in der Verwaltung und bei den Gerichten (Risikobericht) die identifizierten Risiken, die vorgeschlagenen Massnahmen zur Minderung der Risiken und die Restrisiken vollständig und zutreffend beschreibt.**

Nach einleitenden Vorbemerkungen zu M365 und einem Exkurs zu kartellrechtlichen Bedenken der EU zu M365, nimmt der DSB punktuell Vergleiche mit zwei Kantonen und dem Bund vor (Kapitel 2), bevor der DSB Stellung nimmt zum Risikobericht an sich und punktuell zu durch das Projekt identifizierten Restrisiken (Kapitel 3). Es handelt sich um ein umfangreiches und für die Verwaltung des Kantons Luzern weitreichendes, strategisches Vorhaben. Das Projekt hat indes nicht den Auftrag, sich strategischen Risikoüberlegungen zur Einführung von M365 anzunehmen. Verantwortliche Entscheidungsträger können jedoch die Auswirkungen auf die Persönlichkeit oder die Grundrechte der Betroffenen durch Vorhaben wie das vorliegende nicht hinreichend beurteilen, ohne sich der rechtsstaatlichen und strategischen Fragestellungen anzunehmen. Der DSB nimmt deswegen im Rahmen dieser Stellungnahme auch die strategischen Risiken auf (Kapitel 4) und schlägt hierzu Massnahmen vor (Kapitel 5).

2 Vorbemerkungen

2.1 Was ist M365?

M365 ist die Bezeichnung der umfangreichen Cloud-Services von Microsoft. Anstelle der lokal, im eigenen Rechenzentrum betriebenen Anwendungen (On-Premises Software) wird die Software als Service (Software-as-a-Service, SaaS) bei Microsoft bezogen. Es findet damit grundsätzlich keine Installation und IT-Betrieb durch die DIIN statt, sondern die Softwarelösungen sind im Rechenzentrum der Microsoft installiert und werden durch MS betrieben.[2]
Zu den M365 Cloud-Services von Microsoft gehören neben den klassischen MS Office Anwendungen wie Word, PowerPoint oder Excel auch viele weitere Lösungen, insbesondere im Bereich der Kollaboration (Zusammenarbeit) wie Teams für Telefonate und Videokonferenzen, Outlook und Exchange für E-Mails und Datenablagen in der Cloud wie OneDrive oder SharePoint Online. Bei M365 handelt sich also nicht um eine simple Software für die Textverarbeitung oder Tabellenkalkulation, sondern um eine Software-Suite für eine umfassende Büroautomation und Kollaboration. Microsoft bietet diese Software-Suite den Unternehmen und Organisationen als Clouddienst in verschiedenen Enterprise-Lizenzen an. Zudem ist in den Enterprise-Lizenzen auch das Betriebssystem Windows mitlizenziert.

[1] Microsoft Product Terms (Stand 2. Januar 2024), abrufbar unter https://www.microsoft.com/licensing/terms/ (abgerufen am 13.06.2024), SIK Microsoft-Rahmenvertrag für Gemeinwesen 2022 – 2025, und Microsoft Product and Services DPA (Stand 2. Januar 2024), abrufbar unter https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=1 abgerufen am 13.06.2024.
[2] Sehr wohl kann und soll Office 365 (d.h. Word, Excel, Access, PowerPoint, etc.) aktuell lokal installiert und betrieben werden. Hier scheint jedoch ebenfalls absehbar, dass dies nicht längerfristig der Fall sein sollte.

Neu enthalten in den Enterprise-Lizenzen ist auch «Microsoft Copilot for Microsoft 365». Copilot ist eine durch Künstliche Intelligenz (KI) gestützte Assistenzfunktion, die in die Microsoft 365-Anwendungen integriert ist. Es nutzt fortschrittliche KI-Technologien, um Nutzern bei der Erstellung, Bearbeitung und Verwaltung von Inhalten in den verschiedenen Microsoft 365-Programmen zu helfen.

2.2 M365 alles Cloud?

Bis vor etwa 10 Jahren war die Mehrheit der Software von Microsoft lokal installiert, und Kunden erwarben einmalig Lizenzen für Produkte wie Windows, Office und Server-Software. Microsofts Geschäftsmodell basierte auf dem Verkauf dieser Einzellizenzen und periodischen Updates. Dies änderte sich grundlegend mit dem strategischen Schwenk zur Cloud und dem Software-as-a-Service (SaaS)-Modell. Die Anfänge der Cloud-Strategie von Microsoft begannen zwischen 2010 und 2013. Mit der Einführung von Office 365 im Jahr 2011 brachte Microsoft einen Abonnementservice auf den Markt, der cloudbasierten Versionen der traditionellen Office-Anwendungen bot. Dies markierte den Beginn der Transformation hin zu einem SaaS-Modell. Im Jahr 2014 verstärkte Microsoft seinen Fokus auf Cloud-Technologien und erhöhte seine Ausgaben für Forschung und Entwicklung im Cloud-Bereich erheblich, bis hin zur heute praktizierten "Mobile First, Cloud First"-Strategie.
Insgesamt hat Microsoft in den letzten zehn Jahren seine Geschäftsstrategie radikal umgestellt, von einem Modell, das auf dem Verkauf von Einzellizenzen für lokal installierte Software basierte, hin zu einem cloudbasierten SaaS-Modell. Heute ist Microsoft einer der führenden Anbieter von Cloud-Diensten weltweit, mit einem umfassenden Angebot an cloudbasierten Produkten und Dienstleistungen.
Mit dem abonnementsbasierten M365 erwirbt ein Kunde neben den Cloud-Diensten auch lokal installierbare Software wie die klassischen Microsoft Office Produkte Word, Excel, PowerPoint und Outlook aber auch das Betriebssystem Windows. Lange Zeit war unklar, ob diese Killerapplikationen zukünftig weiterhin mit einer einmaligen Lizenz erworben werden können oder nur noch im Abonnement. Microsoft Office 2021 war die letzte Version mit einer dauerhaften Lizenz. Im März 2024 hat Microsoft angekündigt, eine Office 2024 Version anzubieten, welche mit einer Einmallizenz erworben werden kann und für welches der Support für fünf Jahre gewährleistet ist.[3]

2.3 Exkurs: Kartellrechtliche Bedenken zu M365

Im Juli 2023 gab die Europäische Kommission bekannt[4], dass sie eine förmliche Untersuchung bezüglich der Bündelung von Microsoft Teams mit den Suiten Microsoft 365 für Geschäftskunden durch Microsoft eingeleitet hat. Die förmliche Untersuchung soll prüfen, ob Microsoft durch die Kopplung oder Bündelung seiner Kommunikations- und Kollaborationsprodukt Teams gegen die EU-Wettbewerbsregeln verstossen hat, indem es sein Kommunikations- und Kollaborationsprodukt Teams an seine beliebten Unternehmenssuiten Office 365 und Microsoft 365 (M365) gekoppelt hat.
Teams ist ein Cloudbasiertes Kommunikations- und Kollaborationstool. Es bietet Funktionen wie Messaging, Anrufe, Videokonferenzen und Dateifreigabe und vereint Arbeitsplatz-Tools von Microsoft und Drittanbietern sowie andere Anwendungen.
Als Reaktion auf die Ankündigung der formellen Untersuchung durch die Europäische Kommission hat Microsoft Ende August 2023 angekündigt, im Europäischen Wirtschaftsraum und

[3] Upcoming preview of Microsoft Office LTSC 2024 - Microsoft Community Hub abgerufen am 18.06.2024
[4] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_3991/IP_23_3991_EN.pdf, abgerufen am 18.06.2024

der Schweiz die M365 Cloud-Services zukünftig ohne Teams anzubieten.[5] Im April 2024 hat Microsoft angekündigt,[6] die Teams-Plattform weltweit von M365 zu entkoppeln und damit eine Strategie ausgeweitet, die das Unternehmen in Europa eingeführt hatte, um die kartellrechtlichen Bedenken der EU zu zerstreuen.

2.4 Vergleich Kantone und Bund

2.4.1 Bund

Mit dem Projekt Cloud Enabling Büroautomation, kurz CEBA, soll der Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei M365 als neuen Standard in der Bundesverwaltung einführen. Massgeblich wird dies damit begründet, dass die Firma Microsoft die Strategie «Cloud first» verfolgt und Ende 2025 der Lebenszyklus von wichtigen Microsoft-Anwendungen ende. Als Schlüsselprojekt der Bundesverwaltung wird CEBA systematisch durch die Eidgenössische Finanzkontrolle (EFK) geprüft.[7]

Die EFK hat mit Bericht vom 29. Februar 2024 die Prüfung zeitweilen abgeschlossen. Es bemängelt, dass in der Offenlegung der betrieblichen Restrisiken eine durchgängige Transparenz fehle. Eine Einführung der Lösung dürfe erst erfolgen, wenn die organisatorischen und technischen Massnahmen zur Risikominderung wirksam eingeführt sind. Es handle sich hierbei teils um inhärente Risiken eines Cloud-Vorhabens, wie z. B. eine nachrichtendienstliche Ausspähung, Verlust der digitalen Souveränität oder unberechtigte Zugriffe auf vertrauliche Daten, die nicht vollständig beseitigt werden können. Ausserdem seien der EFK auf einer Website des Herstellers Informationen verfügbar, gemäss denen entgegen der einleitenden Prämisse ein weiteres Release der Microsoft Office-Suite zum einmaligen Bezug erfolgen solle (siehe dazu auch Kapitel 2.2, letzter Absatz). Die EFK empfahl dem Bereich DTI, mit Microsoft zu klären, inwieweit und für wie lange mit diesem Release eine Lösung ohne Anbindung an die Cloud möglich bleibe.[8]

Gemäss Mitteilung des DTI wurden die Erkenntnisse der EFK-Prüfung mit den Departementen, namentlich im Digitalisierungsrat Bund, nochmals eingehend besprochen. Die Bundeskanzlei hat auf Basis dieser Diskussionen, in Kenntnisnahme der Restrisiken und nach Einbezug der Generalsekretärenkonferenz den Entscheid getroffen, das Projekt mit den zusätzlich getroffenen Massnahmen weiterzuführen. Der Bundesrat wurde am 14. Februar 2024 über diese Arbeiten, den darauf basierenden Entscheid der Bundeskanzlei sowie die weiteren Schritte informiert.[9]

2.4.2 Kanton Zürich

Der Regierungsrat des Kantons Zürich hat einen Beschluss zur Nutzung von M365 erlassen (RRB 542/2022 vom 30. März 2022[10]). Darin wird festgehalten, dass für die Einführung von Cloud-Lösungen keine Rechtsgrundlagen geändert oder geschaffen werden müssen, sondern

---

[5] https://blogs.microsoft.com/eupolicy/2023/08/31/european-competition-teams-office-microsoft-365/, abgerufen am 18.06.2024.
[6] https://www.microsoft.com/en-us/licensing/news/microsoft365-teams-ww, abgerufen am 18.06.2024.
[7] Vgl. zum Ganzen https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/bueroautomation/projekt-ceba.html abgerufen am 06.06.2024.
[8] Bericht EFK-23740 über die Prüfung des DTI-Schlüsselprojektes Cloud Enabling Büroautomation Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei vom 29. Februar 2024, abrufbar unter https://www.efk.admin.ch/wp-content/uploads/publikationen/berichte/wirtschaft_und_verwaltung/informatikprojekte/23740/23740be-endgueltige-fassung-v04.pdf abgerufen am 18.06.2024.
[9] Informationen DTI zum Stand des DTI-Schlüsselprojektes Cloud Enabling Büroautomation (CEBA) anlässlich Publikation des EFK-Berichts 23740 vom 3. Mai 2024, abrufbar unter https://www.efk.admin.ch/wp-content/uploads/publikationen/berichte/wirtschaft_und_verwaltung/informatikprojekte/23740/kurze-darstellung-zum-aktuellen-stand-pa-23740.pdf abgerufen am 18.06.2024.
[10] https://www.zh.ch/bin/zhweb/publish/regierungsratsbeschluss-unterlagen./2022/542/RRB-2022-0542.pdf abgerufen am 11. Juni 2024.

die geltenden Bestimmungen einzuhalten sind. Demgegenüber wies die Datenschutzbeauftragte des Kantons Zürich früh auf die Notwendigkeit zur Regelung der Rahmenbedingungen für die Auslagerung der Datenbearbeitungen beim digitalen Arbeitsplatz in die Cloud von US-amerikanischen Unternehmen hin. Sie wurde im Rahmen der Arbeiten am Entwurf des Gesetzes über digitale Basisdienste konsultiert und hat Punkte zum Datenschutz eingebracht. Dazu gehört beispielsweise, dass eine Auslagerung der Bearbeitung von besonderen Personendaten in die Microsoft Cloud nicht möglich ist, solange das Unternehmen Zugriff auf die Daten nehmen kann.[11] Die Vernehmlassung über das Gesetz über digitale Basisdienste des Kantons Zürich dauerte bis am 13. Mai 2024.

Zeitgleich hat das Netzwerk Egovpartner, welches Gemeinden und Städte bei der Digitalisierung berät, untersuchen lassen, ob und wie öffentliche Organe im Kanton Zürich M365 des US-amerikanischen Unternehmens Microsoft grundrechtskonform einsetzen können. Die Gutachter Professor Dr. iur. Markus Schefer, Staatsrechtsprofessor der Universität Basel, und Dr. iur. Philip Glass, Lehrbeauftragter der Universität Basel, kommen zum Schluss, dass die Speicherung von Personendaten durch M365 in der Cloud einen schwerwiegenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstelle. Die Daten sämtlicher Personen im Zuständigkeitsbereich des öffentlichen Organs würden durch den Einsatz dieser Cloud-Lösung auf Vorrat zugänglich für US-Behörden. Das öffentliche Organ verliere die Kontrolle über die Daten. Es könne den Anspruch auf Schutz der Betroffenen vor Missbrauch ihrer persönlichen Daten, wie er in der Bundesverfassung festgelegt ist, nicht mehr sicherstellen.[12]

2.4.3 Kanton Bern

Auch der Kanton Bern führt in seiner Verwaltung die M365 ein. Den Wechsel auf M365 begründet der Regierungsrat des Kantons Bern damit, dass Microsoft die lokal installierten Office-Versionen nicht mehr weiter entwickeln wolle. Die neue Lösung aus der Cloud würde ausserdem erweiterte Funktionen für die mobile Arbeit und organisationsübergreifende Zusammenarbeit bieten.[13]

Um den Datenschutz auch in der Cloud sicherzustellen, bleiben die allermeisten Daten der Verwaltung im kantonseigenen Rechenzentrum der Bedag Informatik AG, so auch die E-Mails der Verwaltung. Nur die verwaltungsinterne Zusammenarbeit (Chat, Telefonie, Videokonferenz, Dateiaustausch) erfolge verschlüsselt über die M365-Cloud. Aufbewahrt werden die Cloud-Daten in Schweizer Rechenzentren von Microsoft, und einige Dienstleistungen werden aus Rechenzentren in europäischen Ländern mit einer gleichwertigen Datenschutzgesetzgebung erbracht. Um das Risiko des unbefugten Zugriffs Dritter weiter zu minimieren, dürfen wie in der Bundesverwaltung vorerst keine vertraulichen Informationen oder besonders schützenswerten Personendaten in der M365-Cloud bearbeitet werden.[14]

Die Datenschutzaufsichtsstelle des Kantons Bern hat zum Risikobericht des Amtes für Informatik und Organisation vom 7. Juni 2023 am 16. Juni 2023 Stellung genommen. Eine verlässliche Beurteilung der Wahrscheinlichkeit von US-Behördenzugriffen auf in der Schweiz oder der EU gespeicherte Daten sei deshalb nicht möglich, weil vergangenheitsbasierte Prognosen

[11] https://datenschutz.ch/tb/2023/besondere-risiken-fuer-die-grundrechte-m365, abgerufen am 06.05.2024.
[12] https://datenschutz.ch/tb/2023/besondere-risiken-fuer-die-grundrechte-m365, abgerufen am 06.05.2024. Siehe auch SCHEFER/GLASS, Der grundrechtskonforme Einsatz von M365 durch öffentliche Organe in der Schweiz, eine Analyse am Beispiel des Kantons Zürich, Bern 2023.
[13] https://www.fin.be.ch/de/start.html?newsID=4dcf7269-8143-4744-9951-1bdfeaaf09de, abgerufen am 06.05.2024.
[14] https://www.fin.be.ch/de/start.html?newsID=4dcf7269-8143-4744-9951-1bdfeaaf09de, abgerufen am 06.05.2024.

mehrere Aspekte nicht berücksichtigten. (a) Den CLOUD Act gäbe es erst seit 2018; (b) öffentliche Verwaltungen lagern erst jetzt allmählich Daten in Cloud-Dienste aus; (c) US-Behörden können Microsoft verbieten, betroffene Kunden über den Zugriff zu informieren; (d) in interkontinentalen Verhältnissen kann sich die Zukunft völlig anders entwickeln als aufgrund der Vergangenheit erwartet. Sodann bestehe das Risiko, dass technologiebedingte Risiken von M365 für den Datenschutz und die Informationssicherheit durch den raschen Technologiewandel nicht, unvollständig oder nicht rechtzeitig erkannt würden. Und nicht zuletzt bestehe das Risiko, dass das Vertrauen von Bevölkerung und Wirtschaft in die Sicherstellung des Datenschutzes bei der Digitalisierung der Kantonsverwaltung geschmälert werde, durch Verlust von digitaler Souveränität.[15]

3 Stellungnahme des DSB zu den durch das Projekt identifizierten Restrisiken

Der Risikobericht weist gegenüber dem Regierungsrat sieben Risiken aus, welche nicht durch weitere technische oder organisatorische Massnahmen gemindert werden können (Restrisiken). Bei den Risiken handelt es sich um solche, welche im Rahmen der Risikoanalyse durch das Vorhaben identifiziert wurden. Mit der DSFA ist eine Prognose darüber zu machen, welche Folgen eine geplante Datenbearbeitung für die betroffenen Personen oder Personengruppen aufweist. Wenn sich aus der Abschätzung ergibt, dass die vorgesehene Datenbearbeitung ein hohes Risiko für die Persönlichkeits- oder die Grundrechte der betroffenen Personen zur Folge hat, obwohl rechtliche, technische und organisatorische Massnahmen vorgesehen sind, holt das Organ zum Vorhaben vorab die Stellungnahme des oder der Datenschutzbeauftragten ein, ob eine beabsichtigte Bearbeitung von Personendaten mit dem Datenschutz vereinbar ist (Vorabkonsultation). Ein hohes Risiko besteht insbesondere, wenn für die Datenbearbeitung neue technische Bearbeitungsformen, wesentlich geänderte Prozesse oder ein Abrufverfahren vorgesehen sind oder besonders schützenswerte Personendaten in grossem Umfang oder von mehreren Organen in verknüpften Datenbanken bearbeitet werden.

Mit M365 soll für die Verwaltung und Gerichte eine einheitliche Bürokommunikation und -kollaboration eingeführt werden. Das Vorhaben verweist denn auch auf den Planungsbericht des Regierungsrates an den Kantonsrat vom 29. März 2022 B (108) über die Strategie zur Gestaltung des digitalen Wandels in Wirtschaft, Gesellschaft und öffentlicher Verwaltung. M365 soll die technische Grundlage für eine moderne Kommunikations- und Kollaborationslösung schaffen und wird damit zu einem wesentlichen Element der Datenbearbeitung und der Auftragserfüllung der meisten kantonalen Organe. Der Risikobericht listet in der Ausgangslage den Umfang des Projektes M365 wie folgt aus: Word, Excel und PowerPoint sowie neu, (cloudbasierte) Online-Dienste wie OneDrive und Microsoft Teams. Neben diesen Produkten ist aber auch Exchange Online für E-Mail und Kalender in M365 enthalten und vermutlich wird eine Ablösung von Exchange Server (On-Premises) durch Exchange Online mittelfristig notwendig sein. Da Exchange nicht Teil des Projektes M365 weist der DSB darauf hin, dass bei einem Wechsel von Exchange Server auf den cloudbasierten Exchange Online eine erneute Datenschutz-Folgenabschätzung durchzuführen ist.

[15] Datenschutzaufsichtsstelle (DSA), Restrisiken beim Einsatz von M365 – Stellungnahme zum Bericht an den Regierungsrat vom 16. Juni 2023, abrufbar unter https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj8k5K1wceGAxVrhf0HHavEGVwQFnoECBgQAQ&url=https%3A%2F%2Fwww.dsa.be.ch%2Fcontent%2Fdam%2Fdsa%2Fdokumente%2Fde%2Faktuell%2Fdsa_stellungnahme_zum_risikobericht_m365_de.pdf&usg=AOvVaw0etHaZmkm_I6qS83ZfmBir&opi=89978449 abgerufen am 18.06.2024.

Mit M365 soll laut dem Risikobericht eine Bearbeitung von Daten bis und mit Klassifikationsstufe «vertraulich» möglich sein. Unter vertraulichen Daten werden laut dem Risikobericht auch besonders schützenswerte Personendaten verstanden und Daten, die dem Amts- und Berufsgeheimnis unterliegen oder anderen Geheimhaltungspflichten aus Verträgen oder Spezialgesetzten unterliegen.

Eine Offenlegung von Informationen, welche durch besondere Geheimnisnormen geschützt werden, ist ein Rechtsverstoss und damit nicht nur ein Risiko. Durch die Bearbeitung solcher Daten in M365 manifestiert sich eine Offenlegung – einerseits gegenüber Microsoft selbst, sobald diese nicht durchgehend verschlüsselt sind und/oder Microsoft den Schlüssel dazu hält, andererseits spätestens durch einen nicht autorisierten Zugriff durch Microsoft (wenn nicht bereits aufgrund der inhärenten technischen Zugriffsmöglichkeit). Eine Bearbeitung von Informationen, welche durch besondere Geheimnisnormen geschützt sind, ist auf M365 deshalb nicht erlaubt. Ebenso gilt diese Feststellung für Daten welche dem Berufsgeheimnis unterliegen. Auch diese dürfen nicht mit M365 bearbeitet werden. Schliesslich erachtet der DSB die Bearbeitung von besonders schützenswerten Personendaten durch M365 genauso als nicht datenschutzkonform. Die Triagierung der Daten bis und mit Klassifikationsstufe «vertraulich» ist also aus Perspektive der besonderen Geheimnisnormen und des Datenschutzes untauglich.

Der Risikobericht möchte die Risiken minimieren, indem ein Verbot der Bearbeitung von Dokumenten «die von Interesse für US-amerikanische Behörden oder Gerichte sind» postuliert wird. Mit diesem Verbot und dem «Primat der Fachanwendungen» und soll verhindert werden, dass Daten des Kantons gesetzeswidrig verwendet werden. Es verbleibt bei den Organen und letztendlich auch den Mitarbeitenden zu entscheiden, welche Informationsobjekte von Interesse für US-amerikanische Behörden oder Gerichte sein könnten. Dies scheint dem DSB wenig praktikabel. Genauso wenig wie Mitarbeitenden pflichtwidrige Bearbeitung vorgeworfen werden kann, wenn technische Features den Datenschutz nicht gewährleisten. Es scheint schliesslich illusorisch zu wissen, welche Informationen «von Interesse für US-amerikanische Behörden oder Gerichte» sein sollen, nicht zuletzt da eine solches Interesse ständig ändern kann und die bekanntgegebenen Interessen (z.B. Staatsschutz, Terrorismus- und Verbrechensbekämpfung) stets einer Interpretation bedürfen, meist durch die politische Führung.

Das Vorhaben hat die folgenden sieben Restrisiken identifiziert und weist diese also solche aus:

1. Restrisiko vertragswidriger Datennutzung durch Microsoft
2. Restrisiko Übermittlung von Personendaten in die USA
3. Restrisiko Abhängigkeit von Microsoft
4. Restrisiko Anfragen von US-Strafverfolgungsbehörden an Microsoft
5. Restrisiko mangelnde Transparenz über Telemetriedaten
6. Restrisiko Sublieferanten von Microsoft
7. Restrisiko pflichtwidrige Bearbeitung durch Mitarbeitende

Der DSB nimmt zu den durch das Vorhaben identifizierten Restrisiken dort Stellung, wo er das als notwendig erachtet.

3.1 Restrisiko Abhängigkeit von Microsoft

Das Projekt erachtet das Risiko der Abhängigkeit von Microsoft als keines Risiko. Entgegen der Ausführungen im Risikobericht ist die Eintrittswahrscheinlichkeit einer Abhängigkeit durch das Projekt M365 mit der Inbetriebnahme bereits nahezu realisiert und damit sehr hoch bzw. mit vier von vier zu bewerten. Der zu erwartende Schaden durch eine Abhängigkeit kann weitreichende Konsequenzen haben, weshalb von einem Schadensausmass zwischen zwei bis drei ausgegangen werden muss. Das Risiko der Abhängigkeit von Microsoft erachtet der DSB deshalb im Gegensatz zum Projekt nicht als keines Risiko, sondern als mittleres bis hohes Risiko.

Der Bericht argumentiert, dass Microsoft aller Vorrausicht nach ein Verhalten, das zur Kündigung der Verträge durch Microsofts Kunden führt, unterlassen werde. Der Bericht verkennt in der Bewertung der Abhängigkeit von Microsoft jedoch, dass eben eine solche Kündigung faktisch gar nicht möglich ist. Durch die Einführung der UCC-Lösung Skype for Business von Microsoft für Telefonie, Video und Kollaboration ist die Abhängigkeit noch gestiegen und wird nochmals zunehmen, wenn Microsoft nicht mehr nur Software-Lieferant ist, sondern Dienstleister für die vollständige Bürokommunikation und –kollaboration der kantonalen Verwaltung wird. Ohne aktive Massnahme diese Abhängigkeit zu senken, kann dieses Risiko nicht klein sein. Der DSB stuft dieses Risiko als strategisch ein und geht ausführlich im nachfolgenden Kapitel über die digitale Souveränität und Vendor-Lockin darauf ein.

3.2 Restrisiko Anfragen von US-Strafverfolgungsbehörden an Microsoft

Das ausgewiesene Risiko einer unrechtmässigen Bekanntgabe von Daten durch Microsoft an US-Strafverfolgungsbehörden ist zu klein gefasst. Der US CLOUD Act (Clarifying Lawful Overseas Use of Data Act) wurde 2018 in den USA verabschiedet und regelt den Zugang von US-Behörden zu Daten, die von US-Unternehmen im Ausland gespeichert werden. Dieses Gesetz ermöglicht es US-Behörden, per Gerichtsbeschluss auf Daten zuzugreifen, die sich auf Servern im Ausland befinden, solange diese Daten von US-Unternehmen oder deren Tochtergesellschaften kontrolliert werden, auch wenn diese Daten auf Servern im Ausland gespeichert sind. Die Gerichtsanordnung kann es dem US-Unternehmen auch untersagen, den betroffenen Kunden über die Herausgabeanordnung zu informieren. Nicht zuletzt ist der Kanton Luzern bei einem Verfahren auf Herausgabe nicht Partei und kann auch keine Rechtsmittel dagegen ergreifen. Dies verstösst nicht nur gegen Kantonales Recht, sondern verletzt übergeordnetes Recht. Gewisse private Anwaltskanzleien, welche öffentlich-rechtliche Körperschaften beraten, vertreten die Ansicht, dass mit einem risikobasierten Ansatz die Wahrscheinlichkeit eines solchen Zugriffs berechnet werden kann und wenn diese Wahrscheinlichkeit genügend klein ist, das Risiko akzeptiert werden kann. Die Konferenz der Schweizerischen Datenschutzbeauftragten privatim taxiert die Verletzung von Geheimhaltungsvorschriften ohne anerkannten Rechtfertigungsgrund als rechtliche Schranke der Auslagerung und nicht nur als Risiko.[16]

Neben dem US CLOUD Act existieren zudem noch weitere Gesetze, welche nicht mit der Schweizer Gesetzgebung vereinbar ist. Der Foreign Intelligence Surveillance Act (FISA) der Vereinigten Staaten, speziell die Regelungen unter Section 702, stellt eine zusätzliche und bedeutende Herausforderung für den Datenschutz dar, besonders im Kontext internationaler

[16] prvatim Merkblatt Cloud-spezifische Risiken und Massnahmen, https://www.privatim.ch/wp-content/uploads/2023/10/privatim_Cloud-Merkblatt_v3_01_20220203_def._DE.pdf, abgerufen am 11.06.2024.

Datenübermittlungen. Diese US-Gesetzgebung ermöglicht es amerikanischen Geheimdiensten, die elektronische Kommunikation und andere Daten von Ausländern zu überwachen, die sich ausserhalb der USA befinden, ohne dass dafür einzelne Gerichtsbeschlüsse erforderlich sind. Diese Überwachungsbefugnisse gelten auch für Daten, die auf Servern von US-Unternehmen gespeichert sind, unabhängig von ihrem physischen Standort.

Als Massnahme ist vorgesehen, dass die Bearbeitung von Dokumenten mit Interesse für US-Behörden mit M365 verboten wird. Dies greift aber zu kurz, denn erstens kann einem Mitarbeiter nicht zugemutet werden, dass er bei jeder Bearbeitung von einem Dokument überlegen muss, ob dieses von Interesse für US-Behörden ist und zweitens ist das Interesse für US-Behörden nicht vorhersehbar. Zudem sind auch Randdaten bzw. Telemetriedaten durch US-Behörden zugreifbar. Telefonate von Verwaltungsangestellten, von Polizisten oder von Regierungsratsmitgliedern können somit zwar mit einer Ende-zu-Ende-Verschlüsselung inhaltlich vor dem Zugriff geschützt werden; nicht aber die Verbindungsnachweise (wer hat wann mit wem telefoniert).

4 Strategische Risiken

Der Regierungsratsbeschluss vom 11. Dezember 2007 (Protokoll-Nr. 1609) definierte Microsoft als umfassende strategische Plattform in den Bereichen Betriebssysteme, Datenbanken, Verzeichnisdienste, Büroautomation, Kommunikation, Kollaboration, Workflow, Enterprise Search, Systems und Service Management, Datenaustausch und Portale. Dieser Entscheid war unter den gegebenen Umständen nachvollziehbar und die dannzumal damit verbundenen Risiken vertretbar. Software wurde lokal installiert (On-Premises) und auf der eigenen IT-Infrastruktur betrieben. Dieser Regierungsratsbeschluss vom 11. Dezember 2007, welcher vor Einführung von Office 365 (2011) und weit vor der Cloud-First-Strategie von Microsoft (2014) erfolgte, darf aber nicht unbesehen für die Zukunft und als Freipass für Cloud-Services von Microsoft gelten. Durch den angedachten und umfassenden Einsatz von Microsoft Cloud-Services begibt sich die kantonale Verwaltung in eine Herstellerabhängigkeit von noch nie dagewesenem Ausmass.
Aber auch unabhängig von der digitalen Souveränität ist die durch die mögliche Verletzung von Grundrechten die Rechtsstaatlichkeit gefährdet. Nach dem Legalitätsprinzip bietet das Recht Grundlage und Schranke staatlichen Handelns. Der Eingriff in die Persönlichkeit und die Grundrechte von Betroffenen durch die Verwendung gewisser Cloud-Services von Microsoft ist indes derart gravierend, dass dieser durch die vorliegenden Rechtsgrundlagen nicht getragen werden kann – und zu schaffende Rechtsgrundlagen auf die Vereinbarkeit mit Art. 13 Abs. 2 BV überprüft werden müsste.

4.1 Digitale Souveränität und Vendor Lock-in

4.1.1 Digitale Souveränität

Die Strategie Digitale Verwaltung Schweiz 2024 bis 2027[17] definiert die Digitale Souveränität wie folgt: «Fähigkeit von Bund, Kantonen, Städten und Gemeinden, digitale Behördenleistungen autonom nutzen und kontrollieren zu können. Dabei geht es um die Selbstbestimmung über den gesamten Lebenszyklus eines digitalen Systems, von der Konzeption über die Nutzung bis zur Stilllegung digitaler Systeme und der Daten, die bearbeitet und gespeichert wer-

[17] https://www.fedlex.admin.ch/eli/fga/2024/45/de, abgerufen am 16.05.2024.

den, sowie der daraus resultierenden Prozesse.» Unter den Prinzipien der digitalen Verwaltung soll die Verwaltung auf ihre digitale Souveränität achten, um eine ausreichende und nachhaltige Kontrolle des digitalen Raums zu gewährleisten. Die Strategie nimmt auch Bezug auf Cloud-Lösungen welche das «Cloud-enabled-Government» ermöglichen soll. Im Fokus steht dabei aber die digitale Souveränität (neben anderen Themenfeldern).

Mit der angedachten breiten Nutzung von M365 auf dem Desktop der Kantonsangestellten begibt sich der Kanton Luzern in eine Herstellerabhängigkeit von noch nie dagewesenem Ausmass. Der Kanton ist gegenüber Microsoft weder vertraglich, kommerziell, noch technisch souverän. Die ausgeprägte vertragliche, kommerzielle und technische Fremdbestimmtheit führen dazu, dass die Selbstbestimmung über den gesamten Lebenszyklus nicht gegeben ist. Erschwerend kommt hinzu, dass ein Ausstieg aus M365 im Notfall unmöglich scheint, weil valable Varianten scheinbar nicht geprüft wurden oder nicht vorgesehen sind.

Das Datenschutzrecht geht davon aus, dass eine notwendige Vertragsverhandlung bei einer Auslagerung einer Datenbearbeitung auf Augenhöhe stattfinden kann. Dies ist bei Microsoft bekanntermassen nicht gegeben. Vertragliche Anpassungen sind durch den Kanton Luzern nicht möglich. Auch andere Länder bekunden zunehmend Mühe, von Microsoft verbindliche Informationen und Angaben zu erhalten (siehe dazu Kapitel 4.4., letzter Absatz).

4.1.2 Vendor Lock-in

Vendor Lock-in beschreibt eine Situation, in der ein Kunde stark von einem bestimmten Anbieter (Vendor) abhängig wird und es sehr schwierig oder kostspielig ist, zu einem anderen Anbieter zu wechseln. Dies kann aufgrund verschiedener Faktoren geschehen, einschliesslich:

- *Proprietäre Technologien*

Der Einsatz von Technologien, die nicht standardisiert oder offen sind und daher nicht einfach mit Produkten anderer Anbieter kompatibel sind. Zum Beispiel verwendet Microsoft proprietäre Dateiformate wie .docx, .xlsx und .pptx, die zwar von anderen Programmen geöffnet werden können, aber oft mit Einschränkungen in der Kompatibilität. Dies macht es schwierig, vollständig zu alternativen Lösungen zu wechseln.

- *Integration*

Microsoft-Produkte sind tief integriert, z.B. zwischen Windows, Office und Azure-Diensten. Diese Integration bietet zwar Vorteile in der Nutzung, erschwert aber den Wechsel zu anderen Anbietern.

- *Hohe Wechselkosten*

Die Kosten für den Wechsel zu einem anderen Anbieter sind so hoch, dass sie die potenziellen Vorteile eines Wechsels übersteigen. Dies kann Kosten für neue Lizenzen, Schulungen, Migrationsservices und Datenkonvertierungen umfassen.

- *Vertragsbedingungen*

Verträge, die langfristige Bindungen oder erhebliche Kündigungsstrafen beinhalten, erschweren es, den Anbieter zu wechseln.

- *Integration in bestehende Systeme*

Systeme und Software des Anbieters sind tief in die IT-Infrastruktur des Kunden integriert, sodass ein Wechsel erhebliche technische Herausforderungen und Risiken mit sich bringt.

- *Abhängigkeit von spezifischen Funktionen:*

Der Kunde ist auf bestimmte Funktionen oder Dienstleistungen angewiesen, die nur dieser Anbieter bietet und die nicht einfach durch andere Anbieter repliziert werden können.

- *Schulung und Anpassung*

Mitarbeiter sind oft auf Microsoft-Produkte geschult. Ein Wechsel zu anderen Systemen erfordert umfangreiche Schulungen und Anpassungen der Arbeitsabläufe.
Viele Unternehmensanwendungen sind für Windows entwickelt worden und laufen nicht oder nur eingeschränkt auf anderen Betriebssystemen. Der Wechsel zu einem anderen Betriebssystem wie Linux würde daher erhebliche Anpassungen und möglicherweise neue Softwareentwicklungen erfordern.

Ein Vendor Lock-in kann die Innovationsfähigkeit und Flexibilität einer Organisation einschränken, die IT-Kosten erhöhen und das Risiko von Ausfällen oder Sicherheitsproblemen erhöhen, wenn der Anbieter Probleme hat oder den Service einstellt. Zur Vermeidung von Vendor Lock-in können verschiedene Massnahmen getroffen werden. Namentlich kann der Einsatz von Open Source Software, die keine proprietären Beschränkungen aufweist, helfen die Abhängigkeit von einem einzelnen Anbieter zu vermeiden. Aber auch die Nutzung von standardisierten und offenen Technologien und Schnittstellen, die Interoperabilität und leichten Wechsel ermöglichen. Alternativ kann die Implementierung einer Strategie, die mehrere Anbieter umfasst, Abhängigkeiten reduzieren und Flexibilität erhöhen. Und schliesslich sind massgeblich mit der Vertragsgestaltung langfristige Bindungen oder hohe Hürden zur Kündigung zu vermeiden.

4.1.3 Exkurs: Situation in Deutschland

Im Auftrag des deutschen Bundesministeriums des Innern, für Bau und Heimat (BMI) hat PwC Strategy eine "Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern" erstellt. Der Bericht, der im August 2019 veröffentlicht wurde, untersucht die Abhängigkeiten der Bundesverwaltung von einzelnen Software-Anbietern, insbesondere von Microsoft. Die Analyse zeigt auf, dass eine signifikante Abhängigkeit von Microsoft besteht, da Produkte wie Microsoft Office, Windows und Windows Server weit verbreitet sind. Zum Beispiel verwenden 96 % der unmittelbaren Bundesbehörden Microsoft Office sowie Windows für Arbeitsplatz- und Server-Betriebssysteme. Diese Konzentration führt zu einer starken Abhängigkeit und zu Risiken hinsichtlich der digitalen Souveränität der Bundesverwaltung. Die Studie bewertet die Abhängigkeiten anhand eines definierten Software-Stacks, der verschiedene Ebenen wie Büro-Software, Arbeitsplatz- und Server-Betriebssysteme, Datenbanken und weitere Plattformen umfasst. Die hohe Nutzung von Microsoft-Produkten über mehrere dieser Ebenen hinweg verstärkt die Abhängigkeitsproblematik. Ein Hauptziel der Marktanalyse ist es, Wege aufzuzeigen, wie diese Abhängigkeiten reduziert werden können, um die digitale Souveränität zu stärken. Dies könnte durch den verstärkten Einsatz von Open-Source-Software, die Diversifizierung der genutzten Software-Produkte und die Förderung von Alternativen zu dominierenden Anbietern erreicht werden.

Deutschland hat in den letzten Jahren eine Reihe von Massnahmen ergriffen, um die Abhängigkeit von Microsoft und anderen grossen Software-Anbietern zu verringern und die digitale Souveränität zu stärken. Eine zentrale Initiative ist die Gründung des Zentrums für Digitale Souveränität (ZenDiS) durch den IT-Rat und den CIO Bund. ZenDiS fördert den Einsatz von Open Source Software (OSS) in der öffentlichen Verwaltung und unterstützt die Entwicklung

von alternativen IT-Lösungen. ZenDiS hat verschiedene operative Ziele, darunter die Förderung von Projekten zur Entwicklung bedarfsgerechter OSS-Lösungen für die Verwaltung, die Verbesserung der Rahmenbedingungen für den Einsatz von OSS und die Stärkung des Bewusstseins für die Vorteile von OSS. Das Zentrum agiert als Koordinator und "Trusted Advisor" und vernetzt Akteure auf allen föderalen Ebenen. Ein konkretes Projekt, das durch ZenDiS gefördert wird, ist die Entwicklung eines "souveränen Open Source Software-basierten Arbeitsplatzes" für die öffentliche Verwaltung. Diese Lösung zielt darauf ab, moderne, leistungsfähige und skalierbare Open Source Software bereitzustellen, die den spezifischen Anforderungen der öffentlichen Verwaltung entspricht und Interoperabilität mit bestehenden IT-Systemen gewährleistet. Darüber hinaus wurde eine Strategie zur Stärkung der digitalen Souveränität verabschiedet, die Massnahmen zur Reduzierung der Abhängigkeiten von einzelnen Software-Anbietern und die Förderung eines wettbewerbsfähigen Marktes umfasst. Diese Strategie wurde im Rahmen des IT-Planungsrats erarbeitet und soll die Resilienz und Unabhängigkeit der IT-Systeme der öffentlichen Verwaltung erhöhen.

4.1.4 Vergleich Bundesprojekt CEBA

Das Bundesprojekt CEBA des DTI hat ebenfalls festgestellt, dass der Wechsel in die Cloud zu einem starken Vendor Lock-in führe. Dazu hat CEBA eine Exit-Strategie erstellt und dem Digital Sustainability Lab der Berner Fachhochschule (BFH) den Auftrag erteilt, eine Studie über eine konkrete Umsetzungsmöglichkeit von Alternativsoftware durchzuführen. Dieser Bericht zeigt, dass ein Ausstieg aus der Abhängigkeit von Microsoft im Bereich der Büroautomation mit tauglichen Alternativen bei den Backend Services (wie Ablage (Sharepoint), E-Mail (Exchange) und Echtzeit Kommunikation (Skype for Business, MS-Teams)), den Frontend Services auf dem Client (wie Browser (Edge), MS-Office, Visio, Teams)) möglich sei. In zwei separaten Studien der BFH wurden Alternativen in Open-Source-Software untersucht, mit dem Ergebnis, dass es einerseits für fast alle heute eingesetzten Frontend Services Alternativen gibt, die empfohlen werden können und andererseits für die meisten proprietären Softwarelösungen, die derzeit in der Bundesverwaltung im Bereich der Büroautomation im Einsatz sind, Alternativen für das Backend existieren. Einzig für die "unified communication" («UCC» Skype, Teams) gebe es zwar Alternativen, die würden aber nicht einen gleichwertigen Funktionsumfang bieten.[18]

4.2 Grundrechte und Legalitätsprinzip

Wie in Kapitel 2.4.2 vorerwähnt, untersuchte das Gutachten von Prof. Dr. Markus Schefer und Dr. Philip Glass im Auftrag von egovpartner die Frage, wie die Gemeinden im Kanton Zürich Cloud-Dienste (insbes. M365) verfassungs- und datenschutzkonform nutzen können. Gegenstand der Untersuchung sind die verfassungsrechtlichen Garantien von Art. 13 Abs. 2 BV sowie deren gesetzliche Konkretisierung im Datenschutzrecht und weiteren Erlassen des Kantons Zürich.
Das Gutachten kommt zum Schluss, dass die Speicherung von Personendaten in der Cloud einer US-Anbieterin unfreiwillig «auf Vorrat» zuhanden von U.S.-Behörden erfolge, welche diese mittels CLOUD Act bzw. dem Stored Communications ACT («SCA») u.U. beschaffen könnten, ein spezifisches Eingriffsmoment darstellt, das gemäss Art. 36 BV zu rechtfertigen

[18] STANDTKE/TIEDE, Studie zu Open-Source-Alternativen von Microsoft Services und Produkten in der Schweizerischen Bundesverwaltung Backend-Services vom Februar 2024, abrufbar unter https://www.bk.admin.ch/dam/bk/de/dokumente/dti/themen/CEBA/studie-zu-open-source-alternativen-von-microsoft-services-und-produkten-in-der-schweizerischen-bundesverwaltung-backend-services.pdf.download.pdf/Studie%20zu%20Open-Source-Alternativen%20von%20Microsoft%20Services%20und%20Produkten%20in%20der%20Schweizerischen%20Bundesverwaltung%20Backend-Services.pdf abgerufen am 18.06.2024; STANDTKE/TIEDE, Studie zu Open-Source-Alternativen von Microsoft Services und Produkten in der Schweizerischen Bundesverwaltung Frontend-Services (Client-Anwendungen) vom Februar 2024, abrufbar unter https://www.bk.admin.ch/dam/bk/de/dokumente/dti/themen/CEBA/studie-zu-open-source-alternativen-von-microsoft-services-und-produkten-in-der-schweizerischen-bundesverwaltung-frontend-services.pdf.download.pdf/Studie%20zu%20Open-Source-Alternativen%20von%20Microsoft%20Services%20und%20Produkten%20in%20der%20Schweizerischen%20Bundesverwaltung%20Frontend-Services.pdf abgerufen am 18.06.2024.

ist. Aufgrund der Anzahl der Betroffenen (sämtliche Personen im Zuständigkeitsbereich des Organs) und des faktischen und rechtlichen Kontrollverlusts des öffentlichen Organs ist grundsätzlich von einem schwerwiegenden Eingriff in Art. 13 Abs. 2 BV im Sinne von Art. 36 Abs. 1 Satz 2 BV auszugehen.

Im Hinblick auf die dargelegten Eingriffe und deren Intensität sowie der ungenügenden rechtlichen Grundlage für die Übernahme der korrespondierenden Risiken durch öffentliche Organe im Kanton Zürich muss zum aktuellen Zeitpunkt ein Verzicht auf gewisse Formen der Bearbeitung von besonderen Personendaten mittels M365 empfohlen werden, da diese schwere Eingriffe in die informationelle Selbstbestimmung bedeuteten. Dies betrifft sämtliche Formen der Bearbeitung, die eine Speicherung von Daten in der Cloud von Microsoft umfassen. Hier sei als milderes Mittel auf absehbare Zeit auf die Möglichkeit verwiesen, solche Applikationen auf eigenen Rechenzentren betreiben zu lassen und lediglich die Aktualisierungen über den Clouddienst vorzunehmen. Alternativ kann eine klassische Auslagerung in Rechenzentren eines Dritten, der nicht dem U.S.-amerikanischen Recht untersteht, ins Auge gefasst werden. Diese Einschätzung bleibt im Lichte der künftigen rechtlichen und technischen Entwicklung stetig zu überprüfen.

Der Kanton Luzern plant zur Einführung von M365 eine Klassifikation der Vertraulichkeit von Information in die vier Stufen «öffentlich», «intern», «vertraulich» und «geheim». Geheime Informationen sollen und dürfen nicht mit M365 bearbeitet werden. Der DSB weist darauf hin, dass Informationen, die einer besonderen Geheimnisnorm unterliegen, immer als geheim zu klassifizieren sind. Besondere Geheimnisnorm wurden geschaffen, um das Vertrauensverhältnis zwischen dem Staat bzw. dem Geheimnisträger und der betroffenen Person bzw. dem Geheimnisherren zu schützen. Sie gewähren den Schutz der Grundrechte und der Persönlichkeit der betroffenen Person, deren Personendaten bearbeitet werden. Sie gehen über das Amtsgeheimnis hinaus und gelten – im Unterschied zum «gewöhnlichen» Amtsgeheimnis – absolut. Weil das Organ bei der Entscheidung über die Geheimhaltung der Informationen die Interessen der betroffenen Personen zum Schutz des Vertrauensverhältnisses einbeziehen muss, stehen besondere Amtsgeheimnisse im Ergebnis einer Auslagerung grundsätzlich entgegen, es sein denn, eine technische Lösung unterbindet die Kenntnisnahme durch die Auftragnehmerin bzw. ihre Mitarbeitenden oder diese unterstünden denselben Geheimnisnormen; was, wie vorerwähnt, aufgrund der Konstellation der US-Gesetzgebung nicht möglich ist. Eine solche technische Lösung ist die Chiffrierung von Daten, bei welcher der Schlüssel für die Verschlüsselung nur im Besitz des Kantons ist.

4.3 Wie sicher ist die Cloud von Microsoft?

Im Mai und Juni 2023 kompromittierte ein Bedrohungsakteur die Microsoft Exchange Online-Postfächer von 22 Organisationen und über 500 Einzelpersonen auf der ganzen Welt. Der Akteur griff auf die Konten zu, indem er Authentifizierungs-Tokens verwendete, die mit einem von Microsoft 2016 erstellten Schlüssel signiert waren. Dieses Eindringen kompromittierte hochrangige Vertreter der US-Regierung, die an Angelegenheiten der nationalen Sicherheit arbeiten, einschliesslich der E-Mail-Konten von Handelsministerin Gina Raimondo, des US-Botschafters in der Volksrepublik China, R. Nicholas Burns, und des Kongressabgeordneten Don Bacon.
Signierschlüssel (sog. Master-Keys), die für die sichere Authentifizierung bei entfernten Systemen verwendet werden, sind das kryptografische Äquivalent zu den Kronjuwelen eines jeden Cloud-Dienstanbieters. Wie bei diesem Vorfall geschehen, kann ein Angreifer, der im Besitz

eines gültigen Signierschlüssels ist, sich selbst die Erlaubnis erteilen, auf alle Informationen oder Systeme innerhalb der Domäne dieses Schlüssels zuzugreifen. Die Reichweite eines einzelnen Schlüssels kann enorm sein, und in diesem Fall hatte der gestohlene Schlüssel ausserordentliche Macht. Dieser Signierschlüssel bot den vollständigen Zugriff auf praktisch jedes Exchange Online-Konto überall auf der Welt.

Die Cybersecurity and Infrastructure Security Agency der vereinigten Staaten von Amerika (CISA)[19] untersuchte den Vorfall und publizierte einen ausführlichen Bericht.[20] Der Bericht ist fatal für Microsoft und muss damit in Frage stellen, ob ein internationaler Cloud-Service Provider eine IT-Infrastruktur sicherer betreiben kann als eine Verwaltungsstelle. Der Bericht kommt zum Schluss, dass dieses Eindringen vermeidbar war und niemals hätte stattfinden dürfen. Es hält fest, dass die Sicherheitskultur von Microsoft unzureichend war und grundlegend überarbeitet werden muss.

Der Bericht hält weiter fest, dass eine Reihe von operativen und strategischen Entscheidungen von Microsoft insgesamt auf eine Unternehmenskultur hindeuten, die sowohl Investitionen in die Unternehmenssicherheit als auch ein rigoroses Risikomanagement vernachlässigt. Um den erforderlichen raschen kulturellen Wandel bei Microsoft voranzutreiben, wäre es für die Kunden von Microsoft von Vorteil, wenn sich der CEO und der Verwaltungsrat von Microsoft direkt auf die Sicherheitskultur des Unternehmens konzentrieren und einen Plan mit konkreten Zeitvorgaben für grundlegende, sicherheitsorientierte Reformen im gesamten Unternehmen und in der gesamten Produktpalette entwickeln und öffentlich bekannt geben würden. Und der Bericht empfiehlt, dass der CEO von Microsoft die leitenden Angestellten für die Umsetzung dieses Plans verantwortlich macht. In der Zwischenzeit sollte die Microsoft-Führung in Erwägung ziehen, die internen Microsoft-Teams anzuweisen, die Entwicklung von Funktionen in der gesamten Cloud-Infrastruktur und Produktpalette des Unternehmens zurückzustellen, bis wesentliche Sicherheitsverbesserungen vorgenommen wurden, um einen Wettbewerb um Ressourcen auszuschliessen.

Auch Behörden anderer Länder wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) untersuchen diese Vorfall. Das BSI ist die zentrale Behörde für Fragen der IT-Sicherheit in Deutschland. Es wurde 1991 gegründet und ist dem Bundesministerium des Innern und für Heimat (BMI) unterstellt. Offensichtlich unterstützt aber Microsoft das BSI bei der Untersuchung nicht in dem notwendigen Umfang. Das BSI hat darum den formellen Weg der Anordnung beschritten, weil die Angaben, die das BSI zuvor in einem regulären Austausch erhalten hat, nicht zufriedenstellend waren. Das BSI muss also juristische gegen Microsoft vorgehen, um wichtige Angaben über die verwendete Verschlüsselungstechnologie «Double-Key-Encryption» (DKE) zu erhalten. DKE kann sensible Daten in der Microsoft-Cloud so schützen, dass der Zugriff auf diese Daten auch Microsoft nicht möglich ist. Die Details dazu sind so unklar, dass man beim BSI offenbar nicht einschätzen kann, ob die Angreifer nicht eventuell doch Daten abgreifen kann.

---

[19] CISA ist eine US-amerikanische Behörde, die dem Department of Homeland Security (DHS) unterstellt ist. Sie wurde am 16. November 2018 gegründet und hat die Aufgabe, die Cyber- und Infrastruktur-Sicherheit der Vereinigten Staaten zu verbessern und zu gewährleisten. Die CISA beschäftigt ca. 2'500 Mitarbeiter, teils auch uniformierte Angehörige der Streitkräfte. Für das Geschäftsjahr 2023 hat CISA ein Budget von etwa 2,9 Milliarden US-Dollar. Damit ist die CISA eine der grössten Behörden für Cyber-Security der Welt.

[20] Review of the Summer 2023 Microsoft Exchange Online Intrusion vom 20. März 2024, abrufbar unter https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf abgerufen am 14.06.2024.

Auch der Kanton Luzern wird DKE einsetzen müssen, sollen geheim klassifizierte Daten mit M365 bearbeitet werden. Intransparenz bei Verschlüsselungstechnologie sind der Albtraum eines jeden Sicherheitsexperten.

4.4 Zwischenfazit Strategische Risiken

Es lässt sich feststellen, dass das Vorhaben über die im Risikobericht identifizierten Risiken strategischer Risikoüberlegungen bedarf. Der DSB sieht diese strategischen Risiken vordergründig in der digitalen Souveränität und dem Vendor Lock-in, aber auch in der Frage nach der Rechtsstaatlichkeit, insbesondere also der möglichen Verletzung von Grundrechten und der Frage nach der Einhaltung des Legalitätsprinzips, aber nicht zuletzt auch in der Frage nach der Datensicherheit in der Cloud von Microsoft.

Diesen strategischen Risiken muss nicht das Projekt, sondern vielmehr das zuständige Strategieorgan begegnen. Nach dem Gesagten kann durchaus in Betracht gezogen werden, das Vorhaben nicht oder nicht so zu realisieren. Dafür würden nicht nur die strategischen Risiken an sich sprechen, sondern die festgestellten Alternativen auf verschiedenen Ebenen; sei es in der Technologie an sich, oder sei es an der Produktwahl des Vorhabens, welche aufgrund neuerer Bekanntmachungen durch Microsoft durchaus kurzerhand hinterfragt werden darf. In Anbetracht der Ausrichtung des Vorhabens, konzentriert sich die Stellungnahme nachfolgend jedoch auf die Annahme, dass das Vorhaben wohl realisiert werden möchte.

Bei einer Realisierung des Vorhabens legt der DSB dem Strategieorgan nahe, zu den identifizierten strategischen Risiken auch strategische Massnahmen zu entwickeln. Im Folgenden wird summarisch auf mögliche strategische Massnahmen eingegangen, welche selbstredend auch erst evaluiert und danach auch anders aufgegleist werden können.

5 Strategische Massnahmen

5.1 Digitale Souveränität und Reduktion Vendor Lock-in

Um dem Verlust der digitalen Souveränität und dem Vendor Lock-in gegenüber von Microsoft zu begegnen, ist ein Verbund mehrerer Massnahmen möglich und nötig. Zunächst sieht der DSB dies in der stringenten Reduktion der Abhängigkeit von Microsoft und insbesondere zum Microsoft's Lizenzmodell. Nicht zuletzt hat die Wettbewerbsaufsicht die Verknüpfung zwischen dem Kollaborationsprodukt Teams mit den Unternehmenssuiten Office 365 und Microsoft 365 (M365) kritisiert. Gerade durch die Einführung von Teams und seiner integralen Funktion wird die Abhängigkeit von Microsoft zementiert. Aber auch durch die Erweiterung der Palette von Anwendungen auf M365, reduzieren sich die Möglichkeiten, sich je von Microsoft zu lösen. Es empfiehlt sich deshalb

- eine funktionierende Exit-Strategie zu erarbeiten;
- eine Alternative zu MS Teams zu erwägen;
- keine neuen Apps von M365 nutzen, Alternativen einsetzen; und
- neue Features von M365 wie «Copilot» (künstliche Intelligenz) immer zuerst abschalten und wie auch Erneuerung grundlegender Infrastrukturkomponenten (Microsoft Entra ID, Microsoft Entra Connect Sync) vor einem Einsatz gründlich die Rechtskonformität prüfen (nebst DSFA).

Letztlich steht aber wie mehrfach festgestellt der Kanton nicht alleine mit Problemen der digitalen Souveränität und dem Vendor Lock-in gegenüber von Microsoft da. Microsoft bedient nicht nur Gemeinden und öffentlich-rechtliche Anstalten des Kantons, sondern auch den Bund und andere europäische Länder, mit denen ein Austausch stattfinden oder an denen sich der Kanton orientieren kann. Es empfiehlt sich deshalb

- eine Kooperation mit anderen Kantonen, dem DVS und dem Bund einzugehen; und
- langfristig der Verwaltung einen souveränen digitalen Arbeitsplatz zu gewährleisten.

5.2 Erhalten der Rechtsstaatlichkeit

Es wurde vielerorts festgestellt, dass das Vorhaben schwere Eingriffe in das Grundrecht auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV. Die Intensität dieser Eingriffe lassen sich nicht mit einer genügenden vorhandenen rechtlichen Grundlage tragen. Auch der Kanton Zürich, welcher mit Regierungsratsbeschluss sich für die Übernahme der korrespondierenden Risiken ausgesprochen hat, stellte mittlerweile fest, dass für gewisse Formen der Bearbeitung von besonderen Personendaten durch M365 eine gesetzliche Grundlage notwendig ist. Es empfiehlt sich daher

- in Erwägung des Gutachtens von Prof. Dr. Markus Schefer und Dr. Philip Glass zu evaluieren, wie die kantonale Verwaltung M365 verfassungs- und datenschutzkonform nutzen möchte; und
- mit Blick auf Art. 13 Abs. 2 BV sowie deren gesetzlicher Konkretisierung im Datenschutzrecht und weiteren Erlassen eine gesetzliche Grundlage für einen souveränen, digitalen Arbeitsplatz der kantonalen Verwaltung zu entwerfen und die Datenbearbeitungen dieses Vorhabens damit dem demokratischen Prozess zuzuführen.

Danebst wurden Massnahmen von rechtsstaatlichem Interesse zwar von Microsoft angekündigt, aber nur teilweise vertraglich garantiert. Zusätzlich scheint zweifelhaft, ob diese Massnahmen schliesslich auch durchgesetzt würden. Folglich empfiehlt sich daher

- eine vertragliche Durchsetzung der versprochenen «EU Data Boundary»-Massnahme sicherzustellen; und
- eine vertragliche Durchsetzung der versprochenen «Defend your Data»-Massnahme sicherzustellen.

5.3 Überwachen der Datensicherheit in der Cloud von Microsoft

Angesichts verschiedener schwerwiegender Vorfälle und nicht zuletzt der fatalen Erkenntnisse der CISA in ihrem ausführlichen Bericht hat Microsoft elementare Sicherheitsvorkehrungen zu treffen. Die notwendige Sicherheit ist mitunter nicht nur Grundlage dieses Vorhabens, sondern auch Grundlage für einen entsprechenden Betrieb nach der Realisierung. Es empfiehlt sich daher

- von Microsoft eine Bestätigung der Umsetzung der von CISA verlangten Massnahmen einzuholen; und
- die Vulnerabilität der Sicherheit der Cloud von Microsoft zusammen mit der Exit-Strategie als eigenständiges Risiko im kantonalen Risikomanagement zu überwachen.

6 Fazit

Der DSB hält fest, dass der Risikobericht die identifizierten Risiken, die vorgeschlagenen Massnahmen zur Minderung der Risiken und die Restrisiken zum bezeichneten Stand und im bezeichneten Umfang vollständig und zutreffend beschreibt. Das Vorhaben liegt in einem Spannungsverhältnis von ändernden Vertragsgrundlagen, bevorstehenden Integrationen neuer Funktionen und Erneuerungen grundlegender Infrastrukturkomponenten, welche kontinuierlich die Überwachung der Risiken und die Weiterführung der DSFA erfordern.

Es handelt sich um ein umfangreiches und für die Verwaltung des Kantons Luzern weitreichendes, strategisches Vorhaben. Die gravierenden Auswirkungen auf die Persönlichkeit oder die Grundrechte der Betroffenen durch das Vorhaben erfordern es, sich der rechtsstaatlichen und strategischen Fragestellungen anzunehmen. Der DSB ist der Überzeugung, dass das Vorhaben mit der Übernahme der Restrisiken aus dem Risikobericht durch den Regierungsrat allein nicht realisiert werden kann und darf. Der DSB hat deswegen auch die strategischen Risiken aufgelistet und zu diesen Massnahmen vorgeschlagen:

- *Digitale Souveränität und Reduktion Vendor Lock-in*

Der Kanton Luzern verliert mit dem Vorhaben in Bezug auf für die Erbringung von Behördenleistungen wesentliche Systeme seine digitale Souveränität. Es fehlt eine umsetzbare Exit-Strategie, damit kann auf gewisse Dienstleistungen künftig faktisch nicht verzichtet werden und der Kanton Luzern begibt sich in eine grosse Herstellerabhängigkeit. Gerade durch die Einführung von Teams und seiner integralen Funktion wird die Abhängigkeit von Microsoft zementiert. Ausserdem ist die vieldiskutierte Alternativlosigkeit zu Microsoft-Anwendungen widerlegt und es existieren valable, alternative Services wie auch Kollaborationswerkzeuge. Um dem Verlust der digitalen Souveränität und dem Vendor Lock-in gegenüber von Microsoft zu begegnen, sind Massnahmen möglich und nötig, die Abhängigkeit von Microsoft zu reduzieren. Die digitale Souveränität bleibt nur gewährleistet, wenn der Kanton langfristig der Verwaltung einen souveränen digitalen Arbeitsplatz sicherstellt.

- *Erhalten der Rechtsstaatlichkeit*

Das Vorhaben stellt schwere Eingriffe in das Grundrecht auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV dar. Die Intensität dieser Eingriffe lassen sich nur mit einer genügenden vorhandenen rechtlichen Grundlage rechtfertigen. Aufgrund der Tragweite und dem Bedürfnis, der kantonalen Verwaltung langfristig einen souveränen, digitalen Arbeitsplatz zu entwerfen, erachtet der DSB es als notwendig, das Vorhaben dem demokratischen Prozess zuzuführen. Aber auch unabhängig der gesetzlichen Grundlage, ist als elementare Voraussetzung für das Gelingen des Vorhabens die vertragliche Durchsetzung der «EU Data Boundary»- und «Defend your Data»-Massnahme sicherzustellen.

- *Überwachen der Datensicherheit in der Cloud von Microsoft*

Der Beizug eines internationalen Cloud-Service Providers wie Microsoft ist keine Garantie dafür, dass seine IT-Infrastruktur sicherer betrieben wird. Die notwendige Sicherheit ist mitunter nicht nur Grundlage dieses Vorhabens, sondern auch Grundlage für einen entsprechenden Betrieb nach der Realisierung. Die Vulnerabilität der Sicherheit der Cloud von Microsoft ist daher zusammen mit der Exit-Strategie als eigenständiges Risiko im kantonalen Risikomanagement kontinuierlich zu überwachen.

Zustellung an:
- Regierungsrat des Kantons Luzern
- Projektteam Einführung von M365 in der Kantonalen Verwaltung

Freundliche Grüsse

KANTON LUZERN · DATENSCHUTZBEAUFTRAGTER ·

Matthias R. Schönbächler
MLaw Rechtsanwalt
Datenschutzbeauftragte

Daniel Spichty
MSc ETH
Mitarbeiter Datenschutzbeauftragter