



Bericht an den Stadtrat Olten

Version 1.0

Risiken beim Einsatz von M365

Datum	19.08.2024
Autoren	Teilprojekt Organisation, DigiFit Olten
Programmtitel	DigiFit Olten
Herausgeber	IT-Strategie Board

Inhaltsverzeichnis

1 Zusammenfassung	3
2 Ausgangslage	5
2.1 DigiFit Olten	5
2.2 Der vorliegende Bericht	5
2.3 Eckpunkte der Nutzung von M365 in der Stadtverwaltung	6
2.4 Stand der Einführung von M365 in anderen öffentlichen Verwaltungen	7
3 Risiken, Massnahmen, Restrisiken	8
3.1 Kontrollverlust gegenüber Microsoft	8
3.2 Kontrollverlust gegenüber ausländischen Behörden	10
3.3 Fehlende Transparenz der Bearbeitung von Rand- und Telemetriedaten	11
3.4 Nichteinhaltung von Bearbeitungsvorschriften	12
3.5 Rasche Änderungen der Services durch Microsoft	13
3.6 Rasch wechselnde Subunternehmer von Microsoft	15
3.7 Begrenzte Überprüfbarkeit der Umsetzung der vertraglichen Massnahmen	16
3.8 Abhängigkeit von Microsoft	18

Versionskontrolle

Version	Änderung	Von	Am
0.7	Grundlage Zirkulationsbeschluss IT-Strategie Board	beetroot	18.07.2024
0.8	Beschlossen IT-Strategie Board zhd. Stadtrat Olten	ThJ	09.08.2024
0.9	Änderung Laufprotokoll des Stadtrates vom 19.08.2024	ThJ	19.08.2024
1.0	Genehmigt durch Stadtrat am 19.08.2024, Pro.-Nr. 236	ThJ	19.08.2024

1 Zusammenfassung

Das vorliegende Dokument analysiert zuhanden des Stadtrates der Stadt Olten die Risiken einer Erweiterung der städtischen IT-Infrastruktur mit Microsoft Cloud Services (Microsoft 365) und zeigt Massnahmen zur Minimierung der Risiken auf. Diese Erweiterung ist Teil des Projekts «DigiFit Olten», welches die Stadtverwaltung modernisieren und digitalisieren wird. Der Bericht stellt dar, welche Restrisiken nach vordefinierten Massnahmen verbleiben und vom Stadtrat akzeptiert werden müssen, wenn Microsoft 365 (M365) in der Stadt Olten eingesetzt werden soll.

Im Vergleich zu der heutigen «on premise»- Nutzung von Microsoft-Software, also der Installation dieser Software im eigenen Rechenzentrum, ist diese Erweiterung mit erhöhten Risiken im Bereich der Informationssicherheit und des Datenschutzes verbunden. Aus der Sicht des IT-Strategie Boards sind die identifizierten und formulierten Risiken tragbar. Dies weil die Stadt Olten eine Reihe von sich gegenseitig verstärkenden technischen, organisatorischen und rechtlichen Massnahmen vorsieht, welche die Risiken deutlich reduzieren.

Ausserdem überwiegen die Vorteile einer Migration zu Microsoft Cloud Services, welche die Vision der Stadt Olten, durch moderne Tools eine vernetzte, zeitgemässe Arbeitsumgebung zu schaffen, Arbeitsprozesse zu vereinfachen, Transparenz zu schaffen und sich als attraktiven Arbeitsgeber zu positionieren unterstützt. Diese sind:

- Die Erhöhung der Effizienz, Flexibilität und Skalierbarkeit diverser Ressourcen durch den Zugriff auf eine hochleistungsfähige, sichere und ständig aktualisierte Cloud-Plattform
- Eine zukunftsfähige Arbeitsumgebung, welche einen attraktiven Arbeitsplatz für Fachkräfte darstellt
- Die Verbesserung der Zusammenarbeit und Kommunikation zwischen den Mitarbeitenden, den Direktionen und externen Partnern durch die Nutzung von innovativen und integrierten Tools wie Microsoft Teams, SharePoint oder OneDrive
- Die Vereinfachung der Zugriffe und Berechtigungen auf Daten und Informationen

Ausserdem wäre es riskant, weiterhin auf lokale Office-Software zu setzen, da Microsoft eine «cloud-first»-Strategie verfolgt und den Fortbestand von «on premise»- Applikationen nicht garantiert.

Für sämtliche identifizierte Risiken wurden Massnahmen definiert, welche sich wie folgt zusammenfassen lassen:

- **Massnahmen gegen Kontrollverlust gegenüber Microsoft:** Die Stadt Olten plant, technische, organisatorische und rechtliche Massnahmen zu ergreifen, um zu vermeiden, dass Microsoft auf besonders schützenswerte Daten zugreifen kann. Grundsätzlich ist es untersagt, diese Daten in der M365 Cloud zu bearbeiten und alternative Systeme (z.B. GEVER) werden zur Verfügung gestellt. Für die restlichen Daten gibt es die Möglichkeit der End-to-End-Verschlüsselung für Telefon- und Videogespräche, die Erstellung eines Migrationsplans und eines Datenschutz- und Sicherheitskonzepts, die Schulung der Mitarbeitenden und die Festlegung eines verbindlichen Vertrags mit Microsoft.
- **Massnahmen gegen Kontrollverlust gegenüber ausländischen Behörden:** Die Stadt Olten bezieht die M365-Dienste aus den Schweizer Rechenzentren und ausnahmsweise aus EU-Rechenzentren von Microsoft, so dass die Daten in der Schweiz und in wenigen Fällen möglichst in der EU bearbeitet werden. Microsoft verpflichtet sich vertraglich, die Stadt über Behördenanfragen zu informieren und Daten nur so weit gesetzlich verpflichtet herauszugeben.

- **Massnahmen gegen fehlende Transparenz der Bearbeitung von Rand- und Telemetriedaten:** Microsoft hat vertraglich zugesichert, dass die Rand- und Telemetriedaten, die sie zur Erbringung der M365-Dienste erhebt, pseudonymisiert, minimiert und nicht für andere Zwecke nutzt.
- **Massnahmen gegen Nichteinhaltung von Bearbeitungsvorschriften:** Die Stadt Olten schult die Nutzenden im korrekten Umgang mit besonders schützenswerten Daten und sensibilisiert die Vorgesetzten für die Durchsetzung dieser Weisung. Zudem schult sie die Benutzerinnen und Benutzer in der konformen Nutzung der M365-Dienste und richtet einen digitalen Vereinbarungsprozess für externe Parteien ein.
- **Rasche Änderungen der Services durch Microsoft:** Die Stadt Olten wird die Entwicklung der M365-Dienste laufend beobachten und die Risiken und Massnahmen falls notwendig anpassen.
- **Wechselnde Subunternehmer von Microsoft:** Microsoft kann jederzeit neue oder andere Subunternehmer für die Leistungserbringung einsetzen, die möglicherweise höhere Risiken mit sich bringen. Die Stadt Olten hat kein Recht, den Einsatz solcher Subunternehmer abzulehnen, sondern kann nur den Vertrag mit Microsoft nicht erneuern.
- **Begrenzte Überprüfbarkeit der Umsetzung der vertraglichen Massnahmen:** Die Stadt Olten kann nicht selbst überprüfen, ob Microsoft ihre vertraglichen Pflichten einhält. Die Stadt Olten kann sich aber auf die Fachmedien, die Datenschutzaufsichtsbehörden und andere Kunden von Microsoft stützen, um Hinweise auf Vertragsverletzungen zu erhalten.
- **Abhängigkeit von Microsoft:** Die Stadt Olten wird durch die Nutzung von M365 stärker von Microsoft abhängig, weil die Cloud-Services tiefer in die Verwaltungsabläufe integriert werden. Die Stadt Olten muss die Möglichkeit bewahren, den Lieferanten zu wechseln, wenn die weitere Nutzung von M365 unzumutbar wird.

Mit diesen Massnahmen kann die Stadt Olten von den zahlreichen Vorteilen einer Migration zu Microsoft Cloud Services profitieren und gleichzeitig die Risiken beherrschen.

Der vorliegende Bericht wurde auf der Grundlage des Berichts über Restrisiken beim Einsatz von M365 des Kanton Bern im Rahmen deren Programm work@BE erstellt.

2 Ausgangslage

2.1 DigiFit Olten

Mit dem zurzeit laufenden Projekt DigiFit Olten will die Stadt zukunftsfähige IT-Werkzeuge einführen. Zu den Zielen des Projekts gehört es, die technischen sowie organisatorischen Grundlagen für eine zeitgemässe digitale Zusammenarbeit (Collaboration) zwischen den Direktionen und unter den Mitarbeitenden der Stadt sowie Externen zu schaffen.

Es geht auch darum, die eingesetzte Microsoft-Office-Software auf einen Stand zu bringen, der von Microsoft längerfristig weiter unterstützt wird. Die aktuelle Office-Version «Office 2016» wird nur bis Oktober 2025 unterstützt¹, danach wird der Support dieser Version eingestellt. Daraus und aus den Absichtserklärungen von Microsoft, eine «cloud-first»-Strategie zu verfolgen², ergibt sich, dass es hoch riskant wäre, weiter auf lokale Office-Software zu setzen, deren Fortbestand Microsoft nicht garantiert und der daher zweifelhaft erscheint.

Funktionell und aufwandseitig gleichwertige Alternativen zu Microsoft Office bzw. M365, welche mit weniger Risiken eingeführt werden können, sind nicht bekannt. Entsprechend muss im Rahmen des Projektes die Einführung von M365 an die Hand genommen werden.

2.2 Der vorliegende Bericht

Die Stadt Olten hat für die Einführung von M365 ein Sicherheitskonzept erstellt, welches den Umgang mit der Cloud sowie Schutzmassnahmen für Informationen, Daten und die Infrastruktur definiert. Der vorliegende Bericht fasst in Ergänzung zu diesem Konzept die Risiken bei der Einführung von cloud-basierten Services von Microsoft zusammen und schlägt rechtliche, organisatorische sowie technische Massnahmen zur Reduktion oder Vermeidung dieser Risiken vor.

Bei den geplanten Umsetzungen von spezifischen Business-Anwendungen wie z.B. Einführung eines cloud-basierten Intranets oder Telefonie über MS Teams werden spezifische Vorschriften erarbeitet, welche sich an den Bestimmungen dieses Berichts orientieren sollen. Diese werden dem IT-Strategie Board der Stadt Olten im Auftrag des Sourcing Board zur Kontrolle vorgelegt werden.

In diesem Zusammenhang kam die Direktionskonferenz zum Schluss, dass es aufgrund der Bedeutung der Stadt Olten für die Datenbearbeitungen und die Aufgabenerfüllung der Verwaltung angemessen ist, wenn der Stadtrat als die der Verwaltung vorgesetzte Behörde den Entscheid über die Akzeptanz der Risiken und den Einsatz von M365 fällt.

Der vorliegende Bericht ist die Grundlage dieses Entscheids. Er stellt die Risiken und die Massnahmen für die Einführung von M365 und den Einsatz von cloud-basierten Services dar. Diese sind vom Stadtrat als tragbar zu beurteilen und zu akzeptieren, wenn M365 verwaltungsweit eingeführt werden soll.

Der Grund dafür, dass nicht alle Risiken durch Massnahmen vermieden oder massgeblich reduziert werden können, ist einerseits, dass Microsoft als globaler Dienstleister von Softwarelösungen

¹ Supportzeiträume Office 2016, abgerufen im Dezember 2023: [Microsoft Office 2016 - Microsoft Lifecycle | Microsoft Learn](#)

² [Informationspapier Entscheid CEBA](#), Informationen zur produktiven Nutzung von Microsoft 365, Bundeskanzlei, S. 2

mit übermässig grosser Skalierbarkeit hoch standardisierte Leistungen erbringt, die sie nur beschränkt nationalen und lokalen Anforderungen anpassen will oder kann. Andererseits würden zu viele oder zu weitreichende Massnahmen den Nutzen und die Benutzbarkeit von M365 so sehr einschränken, dass die Angestellten zu sehr in ihrer Arbeit behindert würden. Die im vorliegenden Bericht zusammengefassten Massnahmen versuchen daher, eine möglichst hohe Reduktion von Risiken mit einem möglichst hohen Mehrwert für die Mitarbeitenden in Einklang zu bringen.

Dem risikobasierten Ansatz, den die Stadt Olten damit verfolgt, liegt das kantonale Informations- und Datenschutzgesetz zugrunde, namentlich das Informations- und Datenschutzgesetz des Kantons Solothurn (InfoDG; BGS 114.1³) und die Informations- und Datenschutzverordnung des Kantons Solothurn (InfoDV; BGS 114.2⁴). Ergänzend mit «Richtlinien der Stadt Olten» betreffend Öffentlichkeitsprinzip und Datenschutz (SRO 113).

Die Risikobeurteilung sowie die gestützt darauf ergriffenen Massnahmen, die diesem Bericht zugrunde liegen, beziehen sich auf die Stadt Olten. Sie können nicht unbesehen auf andere Behörden übertragen werden, denn diese bearbeiten andere Daten und müssen teils andere Rechtsgrundlagen beachten. Zudem müssen diese die mit M365 verbundenen Datenschutzrisiken selbst einschätzen. Es ist daher wahrscheinlich, dass andere Behörden, welche M365 einführen, zu einer anderen Einschätzung der Risiken gelangen und nicht dieselben Massnahmen umsetzen wie die hier vorgesehenen.

2.3 Eckpunkte der Nutzung von M365 in der Stadtverwaltung

Die sicherheits-relevanten Eckpunkte der Art und Weise, wie M365 in einer ersten Phase in der Stadt Olten eingesetzt werden soll, sind die folgenden:

- Besonders schützenswerte Daten wie besondere Amtsgeheimnisse, Berufsgeheimnisse sowie den besonders schützenswerten Personendaten werden weiterhin in Fachapplikationen gespeichert und sind von M365 nicht betroffen. Dazu gehören namentlich die Fach- und Verwaltungsapplikationen und ihre Daten, wie beispielsweise die bald eingeführte elektronische Geschäftsverwaltung (GEVER), die Steuerdaten, die Einwohnerkontrolldaten (Dialog GemoWinNG, Dialog G6) sowie Daten der Sozialregion (Diartis KLIBnet).
- Exchange-Postfächer die sensible Daten enthalten werden weiterhin On-Premise betrieben.
- Die M365-Dienste zur Zusammenarbeit (Collaboration) werden primär aus den Schweizer Cloud-Rechenzentren sowie teils aus europäischen Rechenzentren von Microsoft bezogen. Dies sind vor allem die Benutzerverwaltung (Entra ID), die geteilte Dateiablage (OneDrive, Teams, SharePoint), Outlook-Postfächer (Exchange Online) sowie die Videokonferenz-, Telefonie- und Chatlösung (Teams).
- Die Office-Applikationen (Word, Excel, PowerPoint, Outlook, Publisher, Visio, OneNote) werden weiterhin lokal auf den Computern resp. in der Citrix-Umgebung der Mitarbeitenden installiert sind aber für kollaborative Zwecke in der Cloud verfügbar.
- Durch erweiterte Sicherheitsmassnahmen wie Multi-Faktor-Authentifizierung, Gerätemanagement und das Blockieren von Zugriffen aus Ländern und Gebieten ohne angemessenes Datenschutzniveau wird die Microsoft 365 Umgebung der Stadt Olten zusätzlich vor unerwünschten Zugriffen geschützt.

³ Informations- und Datenschutzgesetz (InfoDG) des Kanton Solothurns

⁴ Informations- und Datenschutzverordnung (InfoDV) des Kanton Solothurns

Wichtig ist, dass dieser Lösungsansatz – und damit der vorliegende Bericht – eine Momentaufnahme darstellt. Microsoft entwickelt ihre Dienste laufend weiter, was sowohl eine Zunahme wie auch eine Abnahme von Risiken nach sich ziehen kann. Dieser Umstand ist selbst ein Risiko, auf das im Kapitel 3.5 näher eingegangen wird.

Vor dem Hintergrund dieser raschen Entwicklung wird das IT-Strategie Board die Entwicklung der Services und Risiken laufend beobachten und die Nutzung von M365 sowie die Massnahmen, wenn nötig, anpassen.

Wo sind die Daten der Stadt Olten in M365 genau?

Der Ort von Datenbearbeitungen ist gesetzlich geregelt: Gemäss § 21bis des Datenschutzgesetzes (InfoDG) dürfen Personendaten, von bestimmten Ausnahmen abgesehen, nur im Ausland bearbeitet werden, wenn dort ein angemessener Datenschutz gewährleistet ist. Gemäss der ab 1. September 2023 geltenden Liste in Anhang 1⁵ zur Datenschutzverordnung des Bundes⁶ trifft das auf viele EU- und EWR-Staaten zu, nicht aber auf die USA.

Es ist davon auszugehen, dass der Kanton Solothurn das InfoDG den bundesrechtlichen Vorschriften anpassen wird. In diesem Fall werden die Daten der Stadt Olten in M365 in folgenden Ländern bearbeitet:

- Aufbewahrt (gespeichert) und hauptsächlich bearbeitet werden die Daten in Rechenzentren von Microsoft in der Schweiz.
- Die Daten können auch in anderen Ländern der EU oder des EWR bearbeitet werden, etwa wenn die Schweizer Rechenzentren ausfallen, oder weil bestimmte Leistungen aus anderen europäischen Rechenzentren von Microsoft erbracht werden.
- Nur sehr punktuell und eingeschränkt können einzelne Daten ins aussereuropäische Ausland übermittelt werden, auch in Länder wie die USA, die aus der Sicht der EU- und Schweizer Datenschutzbehörden als datenschutzrechtlich unsicher gelten. Gemäss Microsoft sind dies Daten über bestimmte Supportfälle auf Kundenwunsch sowie Computerprogramme in Dateianhängen, die mutmasslich schädliche Software darstellen und deswegen näher analysiert werden müssen.

2.4 Stand der Einführung von M365 in anderen öffentlichen Verwaltungen

Viele andere öffentliche Verwaltungen in der Schweiz haben M365 eingeführt oder bereiten dies vor. Bekannt sind aktuell folgende Projekte (Stand Dezember 2023):

- Der Bund plant einen hybriden Einsatz von M365, wie im Kanton Bern vorgesehen: Sensitive Informationen werden lokal bearbeitet, andere in der Cloud. Am 15. Februar 2023 hat der Bundesrat der Nutzung von M365 in diesem Sinne zugestimmt.⁷
- Seitens der Kantone haben die Regierungen von AG, NW, SH, SO, ZG und ZH der Einführung von M365 zugestimmt. In den Kantonen AI, BS, BL, FR, GL, LU, OW, SG, UR und VD laufen Projektarbeiten, ist die Einführung im Gang oder schon erfolgt – teils für den Schulbereich, teils für die ganze Verwaltung.⁸

⁵ Verordnung über den Datenschutz: AS 2022 568 - Verordnung vom 31. August 2022 über... | Fedlex (admin.ch)

⁶ Datenschutzverordnung (DSV; SR 235.11)

⁷ «Bund führt Microsoft 365 ein», Medienmitteilung des Bundesrates vom 15. Februar 2023 (<https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-93076.html>)

⁸ Dies ergibt sich aus einer kurzen Recherche öffentlich zugänglicher Informationen: AI wies in der Staatsrechnung 2020 die Kosten der «Neulizenzierung Microsoft M365» aus. BS verfügt über ein Kompetenzzentrum M365. BL und BE erarbeiteten eine Risikoanalyse mit ähnlichen Anforderungen wie der Risiken, Massnahmen, Restrisiken

3 Risiken, Massnahmen, Restrisiken

Dieser Abschnitt stellt die wesentlichen Risiken der Nutzung von M365 vor, ebenso wie die wesentlichen Massnahmen, um die Risiken zu vermeiden oder zu reduzieren, und die verbleibenden Restrisiken.

Die Gliederung der Risiken und Massnahmen erfolgt thematisch, wobei nur dann auf die Eigenheiten der einzelnen M365-Services eingegangen wird, wenn sich diese in Bezug auf Risiken oder Massnahmen wesentlich voneinander unterscheiden. Der Bericht verzichtet bewusst auf eine Quantifizierung des Risikoumfangs (Eintretenswahrscheinlichkeit mal Schadensausmass) der Risiken bzw. Restrisiken mit Zahlen, weil damit in der vorliegenden gerafften Darstellung eine irreführende Scheingenauigkeit verbunden wäre. Stattdessen versucht der Bericht, die Risiken in einer politisch beurteilbaren Art und Weise mit Worten zu umschreiben.

3.1 Kontrollverlust gegenüber Microsoft

Wer Daten durch Dritte bearbeiten lässt (Auftragsdatenbearbeitung), verliert damit einen Teil der Kontrolle über die Daten – also die Möglichkeit, abschliessend wissen und durchsetzen zu können, wer was mit den Daten macht. Das gilt auch für die Nutzung von M365 durch die Stadt Olten.

Die technische und wirtschaftliche Entwicklung der letzten Jahre und Jahrzehnte hat dazu geführt, dass die Nutzung von Cloud-Services von der Ausnahme zur Regel wurde, und zwar sowohl im Privatleben, im Wirtschaftsalltag wie auch bei den Behörden. Die meisten Menschen nutzen ein Android- oder Apple Smartphone, das Chatnachrichten und Fotos in der Cloud speichert. Die meisten Unternehmen nutzen M365 oder vergleichbare Lösungen, oder sind dabei, sie einzuführen. Auch die Behörden könnten ohne die ICT-Leistungen Dritter ihre Aufgaben nicht mehr erfüllen.

Diese Allgegenwart der Cloud darf aber nicht davon ablenken, dass der Kontrollverlust ein Risiko für die betroffenen Personen und Informationen darstellt, denn wer fremde Daten hat, kann sie missbrauchen, verlieren oder sie stehlen lassen. Für behördliche Datenbearbeitungen ist dieses Risiko besonders relevant, weil die Betroffenen anders als im Privat- oder Wirtschaftsleben nicht selbst entscheiden können, ob sie ihre Daten einem Dritten anvertrauen. Daher sieht das InfoDG (insbesondere Art. 15 bis 30) Regeln für die Bearbeitung von Personendaten durch Behörden vor. Sie ist nur zulässig:

- a) wenn es in einem Gesetz oder in einer Verordnung vorgesehen ist;
- b) wenn es nötig ist, um eine auf einem Gesetz oder einer Verordnung beruhende Aufgabe zu erfüllen,
- c) wenn und soweit die betroffene Person die Daten allgemein zugänglich gemacht hat oder
- d) wenn die betroffene Person im Einzelfall eingewilligt hat.

Bei besonders schützenswerten Personendaten gilt zudem verschärft, dass das Gesetz die Bearbeitung ausdrücklich vorsieht oder wenn die Bearbeitung für die Erfüllung einer im Gesetz klar umschriebenen Aufgabe unentbehrlich ist.

Microsoft ist (mit wenigen Ausnahmen, s. unten) technisch in der Lage, die von der Stadt Olten in M365-Cloud-Services bearbeiteten Daten zu lesen, zu verändern oder an Dritte weiterzugeben. Die Daten sind zwar durchgehend verschlüsselt und damit vor dem Zugriff Dritter geschützt, aber Microsoft hat den Schlüssel. Das ist notwendig, damit Microsoft ihre Collaborations-

Dienstleistungen erbringen kann, also es ermöglichen kann, dass Daten und Gespräche team- und organisationsintern geteilt werden.

Es wäre technisch möglich, Alternativen zu prüfen, bei welchen Daten auch gegenüber Microsoft verschlüsselt bleiben. Verschiedene Verwaltungen (z.B. der Kanton Bern) haben eine solche Prüfung durchgeführt, diese aber als unpraktikabel verworfen. Solche Lösungen sind noch kaum praxiserprobt und mit wesentlichen Betriebsrisiken verbunden, weil sie von Microsoft bei der Weiterentwicklung nicht berücksichtigt werden. Sie wären sehr aufwändig zu betreiben und würden eigene Sicherheitsrisiken nach sich ziehen: Fällt der Zugang zum eigenen Schlüssel aus, steht die ganze Verwaltung still. Und vor allem würden solche Lösungen die Zusammenarbeitsmöglichkeiten im Rahmen von M365 massiv einschränken und die verwaltungsinterne Zusammenarbeit deutlich erschweren.

Das Risiko des Kontrollverlusts ist für die Stadt Olten nicht neu. Bei der Nutzung von M365 ergibt sich ein höheres Risiko daraus, dass Microsoft nicht eine stadteigene oder eine Schweizer staatlich beherrschte Unternehmung (wie z.B. Swisscom) ist, sondern eine US-amerikanische Privatunternehmung. Dies reduziert das Mass an Vertrauen, das ihr aus der Sicht der Stadt Olten entgegengebracht werden kann, und wohl auch die Wirksamkeit allfälliger rechtlicher Schritte zur Durchsetzung von Interessen der Stadt Olten. Allerdings ist das Risiko insoweit mit demjenigen vergleichbar, dass die Stadt bereits heute durch die Benutzung anderer Anwendungen eingeht, über welche sie Informationen verarbeitet oder teilt. Beispiele dazu die Sicherheitslösung des amerikanischen Unternehmens Palo Alto Networks Inc. Ausserdem haben bei Telefongesprächen und Videokonferenzen, an denen Personen ausserhalb der Stadtverwaltung beteiligt sind, auch deren Fernmeldedienstanbieter Zugang zu den Gesprächsinhalten.

3.1.1 Massnahmen

Organisatorische Massnahmen:

- Besonders schützenswerte Daten werden nicht in der M365 Cloud bearbeitet. Dazu zählen besonders schützenswerte Personaldaten, besondere Amtsgeheimnisse und Berufsgeheimnisse. Für diesen Zweck wurden klare Richtlinien im Sicherheitskonzept für die Einführung von Microsoft 365 erstellt, welche Daten in welchen Microsoft Applikationen verwendet werden dürfen. Damit beschränkt sich das Risiko des Kontrollverlusts auf Informationen mit geringem Schutzbedarf, wobei allerdings davon ausgegangen werden muss, dass diese Weisung nicht immer eingehalten wird (siehe Kapitel 3.4).
- Die Stadt Olten nutzt M365-Services für Collaboration-Zwecke (E-Mail, Telefon, Video, Chat, Dateiaustausch), nicht aber für die Bearbeitung der grossen Datensammlungen der Verwaltungs- und Fachapplikationen oder für die elektronische Geschäftsverwaltung.
- Die Mitarbeitenden werden bei der Einführung von M365 in der konformen Nutzung der neuen Services geschult und auf den korrekten Umgang mit den Daten und deren Sicherheit sensibilisiert. Dazu wurden klare Richtlinien entwickelt (siehe Sicherheitskonzept für die Einführung von Microsoft 365).

Technische Massnahmen:

- Exchange Postfächer, welche besonders schützenswerte Daten enthalten oder über die entsprechende Daten versendet oder empfangen werden, werden weiterhin On-Premise geführt.
- Für den Versand von besonders schützenswerten Informationen wird der Service IncaMail zur Verfügung gestellt.
- Für Telefon- und Videogespräche (Teams):

- Wenn zwei Personen über Teams ein Telefongespräch oder eine Videokonferenz mit vertraulichen Inhalten führen, können sie die Option «end-to-end encryption» (E2EE)⁹ aktivieren. Dann wird das Gespräch so verschlüsselt, dass auch Microsoft nicht mehr in der Lage ist, es mitzuhören. Diese Option muss jedes Mal manuell aktiviert werden, weil es sonst nicht möglich wäre, Gespräche mit Dritten, die Teams nicht nutzen, zu beginnen oder entgegenzunehmen.
- Organisationseinheiten, die häufig vertrauliche Themen in Videokonferenzen mit mehreren Teams-Nutzenden besprechen, können einen kostenpflichtigen Zusatzdienst¹⁰, der E2EE für Videokonferenzen mit mehreren Teilnehmenden unterstützt, bestellen.

Rechtliche Massnahmen:

- Die allgemeinen Geschäftsbedingungen (AGB) von Microsoft bzw. ihr Data Protection Addendum (DPA)¹¹ und eine Zusatzvereinbarung, die Microsoft für die Schweizer Behörden mit der Digitalen Verwaltung Schweiz (DVS) abgeschlossen hat, verpflichten Microsoft stark zusammengefasst zur sicheren, vertraulichen und zweckgebundenen Bearbeitung aller Daten der Stadt Olten gemäss den Anforderungen des Schweizer Datenschutzrechts. Auf einzelne Vorbehalte wird unten bei den Restrisiken eingegangen.
- Wenn Microsoft vertragswidrig auf Kundendaten zugreift, begehen ihre Mitarbeitenden ggf. Straftaten nach dem Schweizer Recht, sowie nach dem ggf. anwendbaren ausländischen Strafrecht.

3.1.2 Restrisiken

Microsoft ist technisch in der Lage, in Verletzung vertraglicher und gesetzlicher Vorschriften auf die städtischen Daten der Benutzerverwaltung, der Ablagen zum Dateiaustausch, der E-Mails, Chats und (soweit nicht E2EE aktiviert ist) der Telefongespräche und Videokonferenzen der Benutzerinnen und Benutzer zuzugreifen. Diese dürfen weisungsgemäss keine besonders schützenswerten Daten enthalten, jedoch ist es wahrscheinlich, dass diese Weisung nicht immer eingehalten wird.

3.2 Kontrollverlust gegenüber ausländischen Behörden

Sobald Daten der Stadt durch ausländische bzw. ausländisch beherrschte Unternehmen bearbeitet werden, besteht die Möglichkeit, dass die Behörden des betreffenden Staates versuchen, sich für ihre Zwecke Zugang zu diesen Daten zu verschaffen. Weil Microsoft ein amerikanischer Konzern ist, betrifft dies im Kontext von M365 primär die Behörden der Vereinigten Staaten, und konkret zwei US-Bundesgesetze, die einen solchen Zugriff ermöglichen:

Der Foreign Intelligence Surveillance Act (FISA)¹² erlaubt den US-Nachrichtendiensten unter bestimmten Voraussetzungen und unter richterlicher Kontrolle die Nachrichtenbeschaffung durch die Aufklärung elektronischer Übermittlungen. In der Schweiz vermittelt das Nachrichtendienstgesetz dem Nachrichtendienst des Bundes (NDB) vergleichbare Kompetenzen.¹³

Der CLOUD Act¹⁴ erlaubt es US-Strafbehörden, mit richterlicher Genehmigung strafprozessual relevante Informationen von US-Unternehmen einzuverlangen, auch wenn diese ausserhalb der USA aufbewahrt werden¹⁵. Auf diesem Weg könnte Microsoft zur Herausgabe von Oltnen Kundendaten in einem Schweizer Rechenzentrum von Microsoft verpflichtet werden.

⁹ Verwendung der End-to-End Verschlüsselung für Einzelgespräche in MS Teams

¹⁰ End-to-End-Verschlüsselung für vertrauliche Teams-Besprechungen

¹¹ Microsoft Products and Services Data Protection Addendum (DPA)

¹² Kodifiziert in 50 U.S.C. § 1801 ff.

¹³ Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz, NDG) vom 25. September 2015, SR 121; s. etwa Art. 26 Abs. 1 Bst. b: Eindringen in Computersysteme und Computernetzwerke.

¹⁴ Kodifiziert in 18 U.S.C. § 2523 ff.

¹⁵ Vgl. im Einzelnen 18 U.S.C. § 2703

Die Stadt Olten ist nach den hier verfügbaren Informationen kein Hauptziel der US-Nachrichtendienste. Gemäss den hier verfügbaren Informationen versuchen US-Strafbehörden zudem kaum je, wenn überhaupt, strafprozessual relevante Daten über den CLOUD-Act-Prozess (statt über ein Rechtshilfegesuch) aus der Schweiz zu erhalten¹⁶. In Fachkreisen ist man sich uneinig, ob sich die Eintretenswahrscheinlichkeit des Risikos verlässlich beurteilen lässt: Die Datenschutzbehörden verneinen dies, wogegen die verbreitet angewendete Methode von David Rosenthal¹⁷ typischerweise sehr tiefe Eintretenswahrscheinlichkeiten ausweist.

3.2.1 Massnahmen

Organisatorische Massnahmen:

- Nutzung der Microsoft-Rechenzentren in der Schweiz zum Bezug der M365-Dienstleistungen.
- Nutzung der im Aufbau begriffenen Funktion «EU Data Boundary» von Microsoft, so dass die Daten im Übrigen möglichst in der EU bearbeitet werden. Mit der «EU Data Boundary» will Microsoft der europäischen Kundschaft ermöglichen, alle Cloud-Leistungen aus europäischen Rechenzentren zu beziehen, und sicherzustellen, dass ihre Daten Europa nicht verlassen, mit wenigen Ausnahmen (bestimmte Sicherheits- und Supportzwecke, siehe Kapitel 2.3).

Rechtliche Massnahmen:

- Microsoft verpflichtet sich vertraglich zu folgenden Massnahmen:
 - Behörden mit Datenanfragen wenn möglich an ihre Kunden zu verweisen
 - die Kunden über solche Anfragen, wenn zulässig, zu informieren
 - Daten nur soweit gesetzlich verpflichtet herauszugeben
 - behördliche Anfragen, wenn möglich, gerichtlich anzufechten
 - und die betroffenen Personen unter bestimmten Umständen zu entschädigen

3.2.2 Restrisiken

Es ist möglich, dass in voraussichtlich sehr seltenen Einzelfällen städtische Informationen in M365 durch US-Strafverfolgungsbehörden oder Nachrichtendienste eingesehen werden. In M365 dürfen weisungsgemäss nur Sach- und Personendaten bearbeitet werden, jedoch ist es wahrscheinlich, dass diese Weisung nicht immer eingehalten wird (s. Kapitel 3.4).

3.3 Fehlende Transparenz der Bearbeitung von Rand- und Telemetriedaten

Zur Erbringung der M365-Dienstleistungen erhebt Microsoft viele Daten darüber, wie die Dienste genutzt werden. Dazu gehören Informationen wie, wer sich wann einloggt oder wie häufig welche Dienste genutzt werden. Diese Informationen werden teilweise bereits heute unter den aktuellen Lizenzbedingungen erhoben. Diese Daten benötigt Microsoft, um sicherzustellen, dass die Dienste nur im Rahmen der beschafften Lizenzen (d.h. nicht durch zu viele Personen) genutzt werden, um Störungen oder Angriffe auf die Dienste zu erkennen, und um die Dienste weiterzuentwickeln. Die Microsoft-AGB erlauben es Microsoft dementsprechend, Kundendaten auch für «Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind» zu

¹⁶ Gemäss dem «[Law Enforcement Requests Report 2022](#)» von Microsoft hat sie in der letzten verfügbaren Berichtsperiode (1. Halbjahr 2022) in Bezug auf die Schweiz 776 behördliche Herausgabebefragungen erhalten (einschliesslich von Schweizer Behörden), wobei allerdings in keinem Fall tatsächlich Kundendaten herausgegeben wurden. Zudem gibt Microsoft an, dass sie in diesem Zeitraum weltweit keine Daten von Unternehmenskunden ausserhalb der USA an US-Behörden bekanntgab (also die hier interessierende Konstellation).

¹⁷ Cloud-Compliance- und Risk-Assessment für den öffentlichen Sektor in der Schweiz (CCRA-PS), https://www.rosenthal.ch/downloads/Rosenthal_CCRA-PS.xlsx

bearbeiten, nämlich «Abrechnungs- und Kontoverwaltung», «Vergütung», «Interne Berichterstattung und Geschäftsmodellierung» und «Finanzberichterstattung».

Welche solcher Daten Microsoft genau erhebt, und wie sie diese bearbeitet, legt sie gegenüber der Kundschaft nicht vollständig offen. Daraus ergibt sich das Risiko, dass von der Stadtverwaltung bearbeitete Sach- und Personendaten zweckwidrig für eigene Zwecke von Microsoft bearbeitet werden können, und dass die Stadtverwaltung nicht im Einzelnen weiss, welche Daten so bearbeitet werden und wozu. Damit ist auch keine abschliessende Beurteilung darüber möglich, ob diese Datenbearbeitung im Einklang mit dem InfoDG bzw. dem DSG soweit Bearbeitung durch Private erfolgt, steht.

3.3.1 Massnahmen

Rechtliche Massnahmen:

- In ihren AGB sichert Microsoft vertraglich zu, für diese Datenbearbeitung nicht «auf den Inhalt von Kundendaten oder Professional Services-Daten zuzugreifen oder diese zu analysieren», das Prinzip der Datenminimierung einzuhalten, dass die bearbeiteten Daten lediglich «pseudonymisierte Identifikatoren» (also keine Namen) enthalten, und dass die Ergebnisse dieser Bearbeitungen «aggregierte statistische, nicht personenbezogene Daten» sind.¹⁸

3.3.2 Restrisiken

Die Stadt Olten weiss nicht, wie genau Microsoft welche Rand- und Telemetriedaten über die Nutzung der M365-Services durch Angestellte der Stadt bearbeitet. Obwohl Microsoft sich dazu verpflichtet, diese Daten zu pseudonymisieren, ist es nicht ausgeschlossen, dass in bestimmten Fällen eine Depseudonymisierung und damit eine Identifizierung der betroffenen Personen möglich ist.

3.4 Nichteinhaltung von Bearbeitungsvorschriften

Die Stadt Olten verbietet im Grundsatz den Benutzerinnen und Benutzern per Weisung, besonders schützenswerte Daten in Cloud-Diensten zu nutzen. Sie hat dazu Richtlinien erarbeitet und die Informatik-Benutzerweisung aktualisiert, welche für sämtliche Mitarbeitenden zugänglich ist. Ausserdem stellt sie den Benutzerinnen und Benutzern Systeme zur Verfügung, in welchen besonders schützenswerte Daten dem Datenschutzgesetz gerecht bearbeitet werden kann.

Die rechtliche Verbindlichkeit dieser Weisung ergibt sich aus der Zuständigkeit des Stadtrates zum Erlass von Verwaltungsreglementen (Art. 40 Abs. 2 Buchst. f) Gemeindeordnung). Diese Weisung wird den Nutzenden in geeigneter Form vermittelt. Sie ist für alle Benutzerinnen und Benutzer der Stadt Olten verbindlich. Mit externen Parteien wird vor dem Zugriff eine Vereinbarung erstellt (AGB Auslagerung von Informatikdienstleistungen und AGB Datenbearbeitung durch Dritte), bei welchen sie sich den Vorschriften der Stadt Olten verpflichten.

Jedoch ist es wahrscheinlich, dass diese Weisung nicht in allen Fällen eingehalten wird, z.B. aus folgenden Gründen:

- Die Benutzerinnen und Benutzer kennen die Weisung (noch) nicht, etwa im Fall neuer oder externer Mitarbeitenden.

¹⁸ Products and Services DPA (Stand November 2023), S. 8

- Die Benutzerinnen und Benutzer kennen den korrekten Umgang mit besonders schützenswerten Daten (noch) nicht, zumal diese erst im Rahmen von DigiFit Olten verwaltungsweit eingeführt werden.
- Die Benutzerinnen und Benutzer ignorieren die Weisung bewusst, etwa weil es aufwändiger oder zeitraubender wäre, Daten ausserhalb von M365 auszutauschen oder zusammenzuarbeiten.

3.4.1 Massnahmen

Organisatorische Massnahmen:

- Das IT-Strategie Board informiert die Mitarbeitenden laufend im Rahmen der Kommunikation zur Einführung von M365 und im Rahmen von Schulungen über die Bearbeitungsvorschriften.
- Das IT-Strategie Board sensibilisiert namentlich die Vorgesetzten darauf, dass es zu ihrer Führungsverantwortung gehört, diese Sicherheitsvorschriften durchzusetzen, und dass wiederholte oder schwerwiegende Verletzungen zu sanktionieren sind.
- Das IT-Strategie Board prüft, ob es möglich ist, die Benutzerinnen und Benutzern automatisch vor der Nutzung von M365 über die Bearbeitungsvorschriften zu informieren, z.B. mit einem vor der Nutzung erscheinenden «Pop-up»- Fenster.

Technische Massnahmen:

- Vereinbarungsprozess für externe Parteien (Gäste) sollen technisch unterstützt werden, um ein effizientes und sicheres Onboarding der Gäste zu gewährleisten.

3.4.2 Restrisiken

Es ist wahrscheinlich, dass in Einzelfällen weisungswidrig besonders schützenswerte Daten in M365 bearbeitet werden, was die oben ausgewiesenen Risiken erhöht.

3.5 Rasche Änderungen der Services durch Microsoft

Grosse Dienstleister mit hoch skalierbaren Services wie Microsoft entwickeln ihre Cloud-Services in einem hohen Tempo weiter und reichern sie mit immer neuen Funktionen an, um kompetitiv zu bleiben. Das ist für die Kundschaft grundsätzlich ein Vorteil, denn damit werden die Services tendenziell immer besser, ohne dass sich die Kundschaft um die Beschaffung, Installation und Migration neuer Versionen kümmern muss, und ohne, dass sie Wartungsarbeiten wie die Installation von Sicherheitspatches selbst vornehmen muss. Diese rasche Veränderung birgt aber auch Risiken: Es ist z.B. möglich, dass neue Funktionen mit bisherigen Geschäftsprozessen oder bestehender Software der Kundschaft inkompatibel sind, was entsprechende kurzfristige Anpassungen und Folgekosten auslösen kann.

Für diesen Bericht ist vor allem relevant, dass neue Funktionen mit neuen Risiken verbunden sein können, die im Zeitpunkt des nun zu fällenden Einführungsentscheids noch nicht beurteilbar sind. Ein Beispiel dafür ist die absehbare Einführung von Funktionen der generativen künstlichen Intelligenz (KI) in M365:

Ein Beispiel: Funktionen der generativen künstlichen Intelligenz

Generative künstliche Intelligenz (KI) ist eine Technologie, die aus kurzen Eingabetexten («Prompts») sinnvolle Texte, Bilder oder andere Medien erzeugt. Die Basis dieser Outputs sind Computermodelle, die mit äusserst vielen aus dem Internet gesammelten Daten gefüttert wurden. Generative KI ist nicht kreativ, sondern kann nur die ihr bekannten Daten neu zusammensetzen, ähnlich wie ein Kaleidoskop aus Konfetti und Spiegeln immer neue Bilder erzeugt. Seit Anfang

2023 stehen grosse internationale Technologiekonzerne in einem Wettlauf miteinander, um generative KI-Funktionen in ihre Produkte zu integrieren. Wichtige Anbieter und Produkte sind OpenAI (ChatGPT, Bing Chat), Google (Bard) und Bildgeneratoren wie Stable Diffusion und DALL-E.

Viele gehen davon aus, dass diese Technologie die Wissensarbeit und damit die auf ihre basierende Wirtschafts- und Gesellschaftsordnung fundamental verändern wird. Zu den experimentellen oder schon kommerziell verfügbaren Anwendungen gehören:

Übersetzungen

Suchmaschinen, die das Ergebnis als Prosatext statt als Link auf relevante Webseiten ausgeben
Beliebige Texte erzeugen, z.B. bestehende Texte zusammenfassen, oder neue Texte schreiben (wissenschaftliche Arbeiten, Zeitungsartikel, ...)

Bilder und Videos nach Beschreibungen erzeugen

Töne erzeugen, z.B. die Stimme einer bekannten Filmschauspielerin nachbilden

Microsoft hat unter dem Titel «Copilot» Funktionen der generativen KI in ihre Produkte integriert, mit denen z.B. Zusammenfassungen von Dokumenten oder Sitzungsprotokolle automatisch erstellt werden können¹⁹. Solche Funktionen und ihre allfällige Nutzung durch die Stadtverwaltung können Risiken nach sich ziehen:

Es wäre sicherzustellen, dass die KI-Bearbeitung der Oltnen Daten in einem datenschutzrechtlich sicheren Land erfolgt (§ 21^{bis} InfoDG).

Wenn die KI-Systeme Oltnen Daten zum Training ihrer Computermodelle verwenden, könnte dies den Grundsatz der Zweckbindung von Personendaten verletzen, und durch das Einfließen in die Modelle könnten die Daten Dritten, die dieselben Modelle nutzen, zur Kenntnis gelangen. Gemäss Auskunft von Microsoft ist das Training der Modelle anhand von Kundendaten nicht vorgesehen. Die KI-Ergebnisse können plausibel klingen, aber inhaltlich falsch sein (sog. «Halluzination»), was die Benutzenden oft nicht erkennen können.

Bei solchen neuen Technologien wie in diesem Beispiel der Copilot, müssen die Funktionen auf ihre Risiken hin geprüft und geeignete Massnahmen zur Behandlung der Risiken bestimmt werden.

Umgekehrt ist es auch möglich, dass neue Funktionen dazu beitragen, dass bestehende Risiken reduziert werden. Microsoft hat in den letzten Jahren viel darin investiert, den im Vergleich zu den USA viel höheren Datenschutzanforderungen der EU entgegenzukommen (und damit auch der Schweiz, deren Datenschutzrecht sich an dem der EU orientiert). Ein Beispiel dafür ist die oben erwähnte «EU Data Boundary».

3.5.1 Massnahmen

Organisatorische Massnahmen:

- Die Veränderungen von M365 werden laufend beobachtet und beurteilt, um mögliche neue Risiken zu identifizieren. Ausserdem werden neben der Dokumentation von Microsoft auch weitere relevante Quellen wie die Erkenntnisse von Datenschutzbehörden weltweit oder Medienberichte beobachtet. Ein externer Partner wird beauftragt, die Stadt Olten bei diesen Aufgaben zu unterstützen.
- Bei datenschutzrechtlich wesentlichen Änderungen wird sich das IT-Strategie Board mit Hilfe von externen Partnern erneut mit einer Vorabkontrolle befassen und nötigenfalls dem Stadtrat eine angepasste Liste von Restrisiken zum Akzept vorlegen.

¹⁹ [Übersicht über Microsoft Copilot für Microsoft 365 | Microsoft Learn](#)

- Für den Fall, dass die weitere Nutzung von M365 aufgrund neuer Risiken als zu riskant beurteilt wird, bereitet das IT-Strategie Board eine Exit-Strategie vor (siehe Kapitel 3.8.1).

Rechtliche Massnahmen:

Für den Fall, dass die weitere Nutzung von M365 aufgrund neuer Risiken als zu riskant beurteilt wird, hat die Stadt Olten die Möglichkeit den Vertrag über die Nutzung von M365 nicht mehr zu verlängern. Eine Verlängerung muss alle 3 Jahre getätigt werden, ansonsten wird der Vertrag automatisch aufgelöst. Damit werden sämtliche Microsoft-Anwendungen (Word, Excel, PowerPoint etc.) sowie Client- und Serverbetriebssysteme (Windows, Windows Server etc.) nicht mehr zur Verfügung stehen.

3.5.2 Restrisiken

Es ist möglich, dass neue Risiken, die sich zukünftig möglicherweise aus neuen Funktionen von M365 oder einseitigen Vertragsanpassungen von Microsoft ergeben, nicht bzw. spät erkannt werden, oder, dass diese Risiken sich als nicht reduzierbar erweisen.

3.6 Rasch wechselnde Subunternehmer von Microsoft

Microsoft zieht zur Leistungserbringung viele internationale Subunternehmer bei. Darüber informiert sie auf einer Liste im Internet ([Online Services Subprocessors List](#)). Diese Subunternehmer fallen grob in folgende Kategorien:

Subunternehmer, die zur Erbringung bestimmter Leistungen eingesetzt werden, welche die Kundschaft bestellt. Dazu gehört z.B. Accenture, wenn die Kundschaft ihre SAP-Installation in Microsoft-Rechenzentren betreiben will:

Entity Name	Applicable Online Service or Product	Sub-processing Activity	Processing Location(s)	DnB Registered Address	Headquarters	DnB Registered Number	Parent Company
Accenture International Limited	SAP HANA on Azure (Large Instances)	Hardware and software installation and operations	In accordance with the customer-specified regionality of SAP HANA on Azure (Large Instances)	1 Grand Canal Square Dublin 2, Ireland	Ireland	985015354	Accenture Public Limited Company

Subunternehmer, die Microsoft unabhängig von den kundenseitig bestellten Leistungen einsetzt («Any Microsoft Online Service»). Dazu gehören z.B. Supportdienstleister oder «content delivery networks» (CDN) wie z.B. Akamai. Ihre Aufgabe ist es, Microsoft-Inhalte wie Webseiten oder Videos effizient an die Kundschaft zu übermitteln. Diese Übertragung erfolgt gemäss Microsoft so verschlüsselt, dass die CDN die Inhalte nicht einsehen können.

Akamai Technologies, Inc.	Any Microsoft Online Service	Operating Content Delivery Network (CDN) infrastructure to efficiently deliver content	Worldwide	150 Broadway, Cambridge MA, 02142-1413 USA	United States	47775205	Akamai Technologies, Inc.
---------------------------	------------------------------	--	-----------	--	---------------	----------	---------------------------

Personalverleihunternehmen, wie z.B. Accenture, die Microsoft bei Bedarf mit zusätzlichem Personal («contract staff») versorgen. In diesem Fall richten sich der Datenzugriff und der Standort des Personals sowie der Datenbearbeitungsstandort nach den für den jeweiligen Service geltenden Bestimmungen.

Staffing Provider	DnB Registered Address	Headquarters	DnB Registered Number	Parent Company
Accenture International Limited	1 Grand Canal Square Dublin 2, Ireland	Ireland	985015354	Accenture Public Limited Company

Die von Microsoft eingegangenen vertraglichen Verpflichtungen gelten auch für ihre Subunternehmen. Zudem unternimmt Microsoft technische und organisatorische Massnahmen, um den Datenzugriff der Subunternehmen auf das Nötige zu beschränken, und macht ihnen, wenn möglich, nur pseudonymisierte Kundendaten zugänglich (diese Subunternehmen sind in der Liste mit einem Sternchen markiert)²⁰.

Die Risikobeurteilung des Projektes DigiFit Olten ergab, dass die zurzeit ausgewiesenen Subunternehmen (Stand der Liste: 2. Juli 2023), soweit sie für Leistungen an der Stadt Olten überhaupt zum Einsatz gelangen, keine unakzeptablen Risiken zur Folge haben.

Ein Risiko ergibt sich aber daraus, dass Microsoft sich vorbehält, jederzeit neue bzw. andere Subunternehmen beizuziehen. Es ist möglich, dass solche neuen Subunternehmen mit höheren Risiken verbunden sind. In diesem Fall hat die Stadt Olten kein Recht, den Einsatz solcher Subunternehmen abzulehnen, sondern kann lediglich den Vertrag mit Microsoft nach Ablauf des Nutzungsvertrages nicht mehr verlängern.

3.6.1 Massnahmen

Organisatorische Massnahmen:

- Das IT-Strategie Board beobachtet mit Hilfe eines externen Partners im Rahmen der laufenden Überwachung der Weiterentwicklung von M365 (s. Kapitel 3.5.1 oben) auch allfällige Anpassungen der Subunternehmerliste und beurteilt die sich daraus ergebenden Risiken. Es geht mit ihnen wie in Kapitel 3.5.1 oben beschrieben um.

Rechtliche Massnahmen:

- Für den Fall, dass die weitere Nutzung von M365 aufgrund neuer Subunternehmen als zu risikant beurteilt wird, kann die Stadt Olten den Vertrag über die Nutzung von M365 nur nicht verlängern.

3.6.2 Restrisiken

Es ist möglich, dass Microsoft dereinst Subunternehmen beizieht, die aus der Sicht der Stadt ein Risiko darstellen. In diesem Fall kann die Stadt diese Subunternehmen nicht ablehnen, sondern nur den Vertrag nicht verlängern.

3.7 Begrenzte Überprüfbarkeit der Umsetzung der vertraglichen Massnahmen

Microsoft verpflichtet sich zwar, wie oben ausgeführt, vertraglich zur Umsetzung von weitgehenden Massnahmen. Für die Stadt Olten ist die Art und Weise, wie Microsoft ihre Leistungen erbringt, aber nicht transparent; sie kann nicht «hinter die Kulissen» der Rechenzentren und der

²⁰ Vgl. allgemein Microsoft Trust Center, [Microsoft Data Access Management](#), abgerufen 28.12.2023

Softwareentwicklung von Microsoft blicken. Damit kann sie in den meisten Fällen nicht selbst überprüfen, ob Microsoft ihre Verpflichtungen einhält.

Auch dieses Risiko ist bis zu einem bestimmten Grad allen Auftragsdatenbearbeitungen inhärent. Wie bei anderen Auftragsdatenbearbeitungen räumt Microsoft ihrer Kundschaft ein vertragliches Auditrecht ein, das es ihr nötigenfalls erlaubt, die Datenbearbeitung durch unabhängige Fachleute überprüfen zu lassen, und vermittelt der Kundschaft den Zugang zu Microsoft-internen Auditberichten²¹. Im Vergleich zum städtischen Rechenzentrum, Telefoniesystem oder Netzwerk ist die Komplexität der Cloud-Services und der Organisation von Microsoft aber viel höher, was ein wirksames Audit viel teurer und viel schwieriger machen würde.

Der Umstand, dass die Stadt mit M365 einen Service nutzt, der von Millionen von Menschen und hunderttausenden Unternehmen und Behörden weltweit genutzt wird, kann sich zur Überprüfung der Umsetzung der vertraglichen Massnahmen aber als Vorteil auswirken: Die Stadt ist nicht darauf angewiesen, alle möglichen Umsetzungsdefizite selbst erkennen und nachweisen zu müssen. Vielmehr kann sie die Synergien nutzen, die sich daraus ergeben, dass die globalen Fachmedien, viele Datenschutzaufsichtsbehörden und viele andere Kunden mit ähnlichen oder höheren Sicherheits- und Datenschutzerfordernungen die Leistungserbringung durch Microsoft ebenfalls aktiv im Auge behalten.

3.7.1 Massnahmen

Organisatorische Massnahmen:

- Das IT-Strategie Board beobachtet mit Hilfe eines externen Partners im Rahmen der laufenden Überwachung der Weiterentwicklung von M365 (siehe Punkt 3.5.1) auch allfällige Hinweise darauf, dass Microsoft ihre vertraglichen Pflichten nicht umsetzt. Es behält dazu insbesondere die Fachmedien und die Berichte von Aufsichtsbehörden weltweit im Auge.
- Wenn Hinweise darauf bestehen, dass Microsoft ihre vertraglichen Pflichten nicht umsetzt, vernetzt sich das IT-Strategie Board mit anderen Grosskunden von M365, primär anderen öffentlichen Verwaltungen der Schweiz z.B. via Digitale Verwaltung Schweiz, mit dem Ziel, ein gemeinsames Vorgehen gegenüber Microsoft festzulegen, z.B. die gemeinsame Durchführung und Finanzierung eines Audits.

Rechtliche Massnahmen:

- Wenn ernsthafte Hinweise auf Vertragsverletzungen seitens Microsofts bestehen, prüft das IT-Strategie Board die Ausübung des vertraglichen Auditrechts im Verbund mit anderen M365-Grosskunden.
- Wenn Vertragsverletzungen festgestellt sind und anhalten, prüft das IT-Strategie Board die gerichtliche Durchsetzung des Vertrags, die Geltendmachung von Schadenersatzansprüchen oder die Kündigung der Vertragsbeziehung.

3.7.2 Restrisiken

Es ist möglich, dass Microsoft seine vertraglichen Verpflichtungen verletzt, ohne dass die Stadt das (zeitnah) weiss.

²¹ DPA vom 15. November 2023, S. 9, Abschnitt «Prüfung der Einhaltung»

3.8 Abhängigkeit von Microsoft

Jede geschäftliche Nutzung von Software führt zu einer mehr oder weniger grossen Abhängigkeit vom Hersteller der Software, denn es ist teuer und aufwändig, eine einmal eingeführte Software auszuwechseln: Daten müssen migriert, Prozesse angepasst und Mitarbeitende geschult werden. Und ein solches Projekt ist mit dem Risiko des Scheiterns oder von Verzögerungen verbunden, mit entsprechenden Auswirkungen auf die Geschäftsprozesse. Wie andere Grossunternehmen steht die Stadt Olten bereits in einem solchen Abhängigkeitsverhältnis zu wichtigen Softwarelieferanten wie Dialog oder Microsoft. Mit der Einführung von M365 verstärkt sich dieses Abhängigkeitsverhältnis, denn die zu M365 gehörenden Collaboration-Lösungen von Microsoft werden im Zuge der fortschreitenden Digitalisierung voraussichtlich tiefer in die städtische Verwaltungsabläufe integriert, als dies bei den bisherigen Lösungen der Fall war.

Gleichzeitig muss die Stadt nach Möglichkeit die Handlungsfreiheit bewahren, den Lieferanten nötigenfalls zu wechseln und eine Alternative zu M365 einzuführen, sollte je eine Situation eintreten, die eine weitere Nutzung von M365 verunmöglichen würde. Solche Situationen sind möglich und können ihren Ursprung in untragbarer Preissteigerung der Lizenzgebühren, gewichtigen Sicherheits- oder Datenschutzdefiziten, oder geänderten rechtlichen und politischen Rahmenbedingungen haben.

3.8.1 Massnahmen

Organisatorische Massnahmen:

- Wenn es sich abzeichnet, dass die Zusammenarbeit mit Microsoft beendet werden soll, kann eine Exit-Strategie entwickelt werden. Angesichts der kontinuierlich sich wandelnden Software-Umgebungen entscheidet sich die Stadt Olten dafür, auf eine detaillierte Ausarbeitung einer Exit-Strategie zum aktuellen Zeitpunkt zu verzichten.
- Besonders schützenswerte Personendaten wären im Fall einer Exit-Strategie nicht betroffen, da sie nicht in M365 abgelegt werden (siehe Punkt 2.3 Eckpunkte der Nutzung von M365 in der Stadtverwaltung). Daher wären ein Teil der wichtigen Informationen weiterhin in Fachapplikationen verfügbar.

Technische Massnahmen:

- Es werden Sicherungs-Optionen geprüft, bei welchen alle M365-Daten bei einem Schweizer Cloud-Anbieter gesichert werden können, welcher ausschliesslich dem Schweizer Recht untersteht (z.B. Mount10 AG). Zugriff auf die meisten Daten ist in einem solchen Fall mit nicht-Microsoft-Anwendungen möglich.

3.8.2 Restrisiken

Für den Fall, dass die Stadt Olten sich dereinst gezwungen sehen sollte, die Nutzung von M365 relativ kurzfristig einzustellen, wird der Wechsel zu einer Alternativlösung hohe Kosten und viel Aufwand in der Verwaltung auslösen und mit zumindest vorübergehenden Einschränkungen in der Abwicklung der Verwaltungsabläufe verbunden sein. Dies besonders darum, weil Microsoft Anwendungen wie Word, Excel, PowerPoint etc. von einer Exit-Strategie auch betroffen sein werden.

AUSZUG AUS DEM PROTOKOLL DES STADTRATES VON OLTEN

Vom 19. August 2024

Prot.-Nr. 236

Projekt Digifit Olten, Risikobericht Einsatz von MS 365 Online/Genehmigung

Im Rahmen der Umsetzung der IT-Strategie und der damit verbundenen Nutzung von Kollaborationslösungen, welche ein vernetzteres und flexibleres Arbeiten ermöglichen, werden auch Instrumente zum Einsatz kommen, welche z.B eine Datenhaltung nicht mehr nur auf eigenen Systemen, sondern sogenannte Cloud-Speichern vorsehen.

Im Weiteren ist in der heutigen Arbeitswelt vieles von der Firma Microsoft abhängig. Mit der Einführung von Microsoft Office 365 Online wird die Abhängigkeit nochmals ein Stück grösser.

Das IT-Strategieboard ist überzeugt, dass der eingeschlagene Weg, wie ihn nun auch diverse kantonale Verwaltungen gehen, der richtige Weg ist. Die mit diesem Weg verbundenen Risiken werden in beiliegendem Bericht transparent aufgezeigt und sollen vom Stadtrat als oberstem Organ der Stadtverwaltung genehmigt werden.

Beschluss:

1. Der Stadtrat genehmigt den Risikobericht zum Einsatz von Microsoft M365 Online und akzeptiert die dargelegten Risiken.
2. Das IT-Strategieboard wird mit der Umsetzung beauftragt.

Mitteilung an:
Direktion Finanzen und Dienste, IT, Thomas Jost
Finanzverwaltung, Urs Tanner

Stadtkanzlei Olten
Der Stadtschreiber:

