Kanton Bern
Canton de Berne

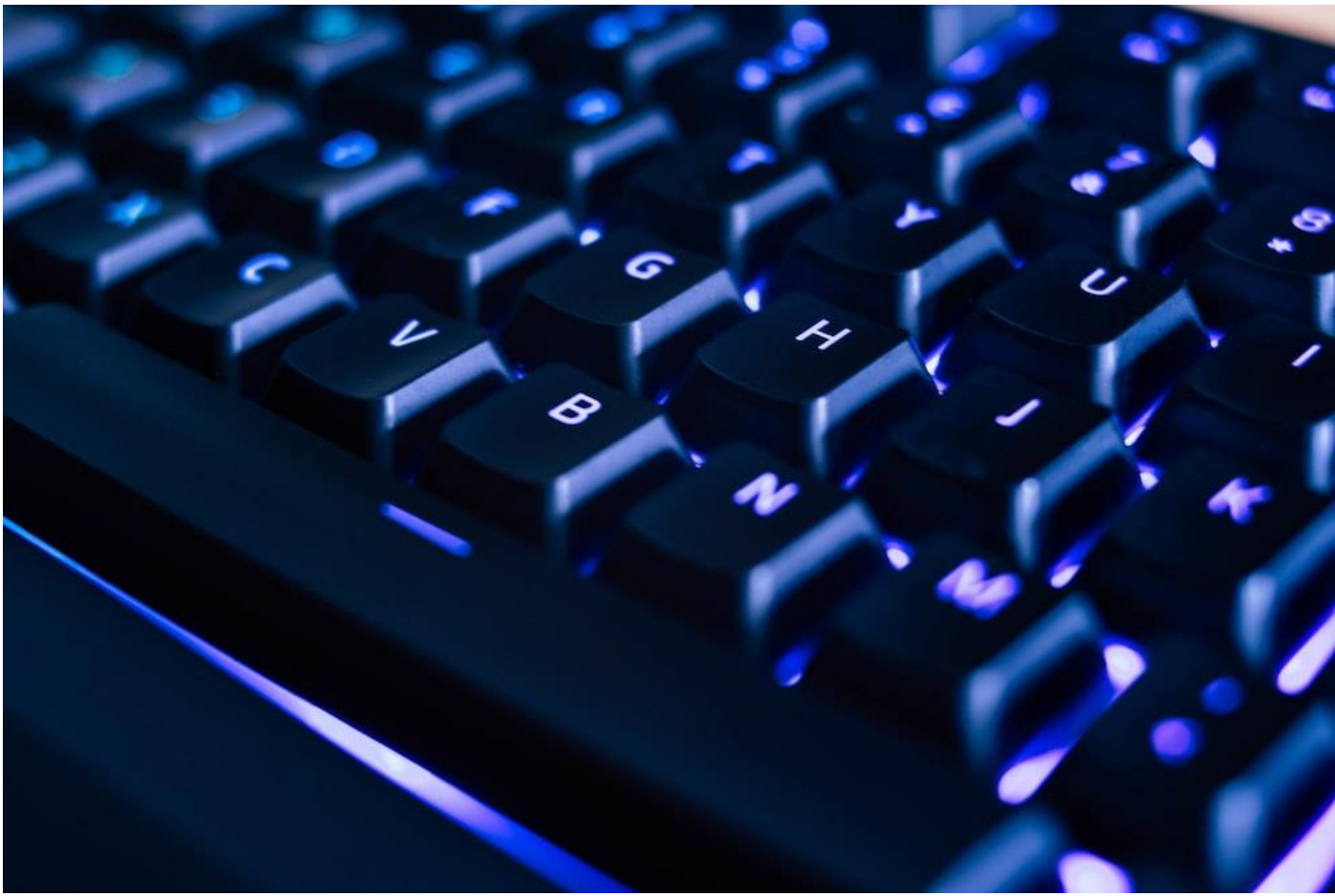
Programm work@BE

Restrisiken beim Einsatz von M365

Bericht an den Regierungsrat

Bearbeitungsdatum	7. Juni 2023
Version	1.0
Dokument Status	fertiggestellt
Klassifizierung	Nicht klassifiziert
Autor/-in	Thomas Fischer
Dateiname	Restrisiken beim Einsatz vom M365, Bericht
Dokumentnummer	99085710
Geschäftsnummer	2021.KAIO.530
Geschäftstitel	PRJ0091352 work@BE

Herausgeber: Amt für Informatik und Organisation (KAIO)



Inhaltsverzeichnis

1. Zusammenfassung

Ab Mitte 2023 will die Kantonsverwaltung die cloudbasierten Services «Microsoft 365» (M365) für die ICT-Grundversorgung der Verwaltung einsetzen. Dies ist im Vergleich zu der heutigen «on premise»-Nutzung von Microsoft-Software, also der Installation dieser Software im eigenen Rechenzentrum, mit erhöhten Risiken im Bereich der Informationssicherheit und des Datenschutzes (ISDS) verbunden.

Der vorliegende Bericht zeigt zuhanden des Regierungsrates auf, welche Massnahmen das Amt für Informatik und Organisation (KAIO) unternimmt, um diese Risiken zu vermeiden oder zu reduzieren. Er stellt auch dar, welche Restrisiken nach diesen Massnahmen verbleiben und akzeptiert werden müssen, wenn M365 in der Kantonsverwaltung eingesetzt werden soll.

Aus der Sicht des KAIO sind diese mit der Datenschutzaufsichtsstelle (DSA) zusammen identifizierten und formulierten Restrisiken tragbar. Dies, weil der Kanton Bern, insbesondere im Vergleich zu anderen öffentlichen und privaten Organisationen, die M365 nutzen, in enger Abstimmung mit der DSA eine Reihe von sich gegenseitig verstärkenden technischen, organisatorischen und rechtlichen Massnahmen vorsieht, welche die Risiken deutlich reduzieren.

Nach diesen Massnahmen verbleiben im Wesentlichen folgende Restrisiken:

1. **Kontrollverlust gegenüber Microsoft:** Microsoft ist technisch in der Lage, in Verletzung vertraglicher und gesetzlicher Vorschriften auf die kantonalen Daten der Benutzerverwaltung, der Ablagen zum Dateiaustausch, der Chats und (soweit nicht die End-to-End-Verschlüsselung aktiviert ist) der Telefongespräche und Videokonferenzen der kantonalen Behörden zuzugreifen.

2. **Kontrollverlust gegenüber ausländischen Behörden:** Es ist möglich, dass in voraussichtlich sehr seltenen Einzelfällen kantonale Informationen in M365 durch US-Strafverfolgungsbehörden oder Nachrichtendienste eingesehen werden.

3. **Fehlende Transparenz der Bearbeitung von Rand- und Telemetriedaten:** Der Kanton weiss nicht, wie genau Microsoft welche Rand- und Telemetriedaten über die Nutzung der M365-Services durch Angestellte des Kantons 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.

4. **Nichteinhaltung von Bearbeitungsvorschriften:** Um die vorstehenden Risiken zu mitigieren, werden die Mitarbeitenden angewiesen, nur Inhalte mit geringem Schutzbedarf in M365 zu bearbeiten. Es ist aber wahrscheinlich, dass in Einzelfällen dennoch weisungswidrig schützenswerte Inhalte in M365 bearbeitet werden, was die oben ausgewiesenen Risiken erhöht.

5. **Rasche Änderungen der Services durch Microsoft:** Microsoft entwickelt ihre Services rasch weiter und führt häufig neue Funktionen ein. Diese können mit zusätzlichen ISDS-Risiken verbunden sein, wie z.B. Funktionen der generativen künstlichen Intelligenz. Es ist möglich, dass solche neuen Risiken nicht bzw. spät erkannt werden, oder dass sie sich als nicht mitigierbar erweisen.

6. **Rasch wechselnde Subunternehmer von Microsoft:** Microsoft zieht zur Leistungserbringung (z.B. Support, Datenübermittlung) viele internationale Subunternehmer bei und informiert darüber auf einer Liste im Internet. Es ist möglich, dass Microsoft dereinst Subunternehmer beizieht, die aus der Sicht des Kantons ein ISDS-Risiko darstellen. In diesem Fall kann der Kanton diese Subunternehmer nicht ablehnen, sondern nur den Vertrag kündigen.

7. **Begrenzte Überprüfbarkeit der Umsetzung der vertraglichen Massnahmen:** Weil Microsofts Systeme und interne Prozesse für die Kundschaft nicht transparent sind, ist es nur schwierig möglich, zu überprüfen, ob Microsoft die vertraglichen Verpflichtungen z.B. hinsichtlich des Zwecks und des Orts von Datenbearbeitungen einhält. Es ist daher möglich, dass Microsoft diese Verpflichtungen verletzt, ohne dass der Kanton das (zeitnah) weiss.

8. **Abhängigkeit von Microsoft:** Für den Fall, dass der Kanton 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.

2. Ausgangslage

2.1 Programm work@BE

Mit dem zurzeit laufenden Programm work@BE wollen das KAIO und die kantonseigene Bedag Informatik AG (Bedag) den PC-Arbeitsplatz der Kantonsverwaltung (BE-KWP) vollständig erneuern. Zu den Zielen des Programms gehört es, die technischen Grundlagen für eine zeitgemässe digitale Zusammenarbeit (Collaboration) unter den Kantonsmitarbeitenden zu schaffen, und die Anforderungen des Grossen Rates an seinen eigenen Arbeitsplatz gemäss der Motion 094-2022 «IT-Infrastruktur und Internet/Informationsangebot zum Grossen Rat und seinen Organen» umzusetzen.

Vor allem aber geht es darum, die eingesetzte Microsoft-Office-Software auf einen Stand zu bringen, der von Microsoft längerfristig weiter unterstützt wird. Die aktuelle lokale Office-Version «Office 2021» wird nur bis 2026 unterstützt[1], und eine spätere Version ist nicht angekündigt. Daraus und aus den Absichtserklärungen von Microsoft, eine «cloud first»-Strategie zu verfolgen[2], ergibt sich, dass es hoch riskant wäre, weiter auf lokale Office-Software zu setzen, deren Fortbestand Microsoft nicht garantiert und der daher zweifelhaft erscheint.

Nachdem die Abklärungen des Programms ergaben, dass es für den Kanton zurzeit keine risikoarm einführbare und funktionell gleichwertige Alternative zu Microsoft Office bzw. M365 gibt, muss das Programm die Einführung von M365 in der Kantonsverwaltung an die Hand nehmen.

2.2 Der vorliegende Bericht

In Umsetzung der kantonalen ISDS-Vorschriften hat das Programm für die einzelnen Microsoft-Services, die genutzt werden sollen, ISDS-Konzepte erstellt. Diese identifizieren die mit der Nutzung der Services verbundenen ISDS-Risiken, legen Massnahmen zur Reduktion oder Vermeidung dieser Risiken vorgesehenen Massnahmen fest und weisen die verbleibenden Restrisiken aus. Diese ISDS-Konzepte hat das KAIO wie gesetzlich vorgeschrieben der Datenschutzaufsichtsstelle des Kantons Bern (DSA) zur Vorabkontrolle vorgelegt.[3] In diesem Zusammenhang kamen die DSA und das KAIO überein, dass es aufgrund der Bedeutung des BE-KWP für die Datenbearbeitungen und die Aufgabenerfüllung der Kantonsverwaltung angemessen ist, wenn der Regierungsrat als die der Verwaltung vorgesetzte Behörde den Entscheid über die Akzeptanz der Restrisiken und den Einsatz von M365 fällt.

Der vorliegende Bericht ist die Grundlage dieses Entscheids. Er ist eine Zusammenfassung der ISDS-Konzepte und der Befunde der DSA zu diesen Konzepten aus dem Vorabkontrollverfahren. Er stellt die

[1] Supportzeiträume Office 2021, Microsoft, abgerufen im Juni 2021
[2] Informationspapier Entscheid CEBA, Informationen zur produktiven Nutzung von Microsoft 365, Bundeskanzlei, S. 2
[3] Art. 17a des Datenschutzgesetzes (KDSG, BSG 152.04) vom 19.02.1986

ISDS-Risiken und die ISDS-Massnahmen jedoch nicht umfassend dar, sondern beschränkt sich auf diejenigen gewichtigen Risiken, die nach dem Ergreifen angemessener Sicherheitsmassnahmen verbleiben. Diese sind vom Regierungsrat 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 Hyperscaling-Dienstleister 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 Kantonsangestellten und Behördenmitglieder zu sehr in ihrer Arbeit behindert würden. Die im vorliegenden Bericht zusammengefassten Massnahmen versuchen daher, eine möglichst hohe Reduktion von ISDS-Risiken mit einem möglichst hohen Mehrwert für die Mitarbeitenden in Einklang zu bringen.

Der risikobasierte Ansatz, den der Kanton Bern damit verfolgt, liegt der neueren nationalen und kantonalen ISDS-Gesetzgebung zugrunde, namentlich den Entwürfen für die Totalrevision des Datenschutzgesetzes (KDSG; BSG 152.04) und für ein kantonales Gesetz über die Informations- und Cybersicherheit (ICSG).

Die Risikobeurteilung sowie die gestützt darauf ergriffenen Massnahmen, die diesem Bericht zugrunde liegen, beziehen sich auf die Kantonsverwaltung. Sie können nicht unbesehen auf andere Behörden (wie Gemeinden, Bildungs- oder Gesundheitsorganisationen) 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 Berner 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 Kantonsverwaltung

Die ISDS-relevanten Eckpunkte der Art und Weise, wie M365 in einer ersten Phase im Kanton Bern eingesetzt werden soll, sind die folgenden:

- Die meisten und wichtigen Daten der Kantonsverwaltung werden weiterhin im Rechenzentrum der kantonseigenen Bedag gespeichert und sind von M365 nicht betroffen. Dazu gehören namentlich die Fach- und Konzernapplikationen und ihre Daten, wie etwa die elektronische Geschäftsverwaltung (GEVER), die Steuerdaten (NESKO), die Einwohnerkontrolldaten (GERES) und die Strassenverkehrsdaten (SUSA) sowie die E-Mails der mit der kantonalen E-Mail-Adresse versendeten bzw. erhaltenen Nachrichten.

- Die Office-Applikationen (Word, Excel, PowerPoint, Outlook) werden weiterhin lokal auf den Computern der Mitarbeitenden installiert und werden nicht aus der Cloud genutzt. Das heisst, dass Word-Dokumente, Excel-Tabellen etc. normalerweise nicht in der Cloud bearbeitet werden, ausser die Nutzenden verschieben sie bewusst in eine Cloud-Umgebung, um etwa die Zusammenarbeit mit anderen Personen zu ermöglichen.

- Nur die Dienste zur Zusammenarbeit (Collaboration) werden primär aus dem Schweizer Cloud-Rechenzentrum sowie teils aus europäischen Rechenzentren von Microsoft bezogen. Dies sind vor allem die Benutzerverwaltung (Azure AD), die geteilte Dateiablage (OneDrive) sowie die Videokonferenz-, Telefonie- und Chatlösung (Teams). Allerdings wird den Nutzenden verboten, diese Cloud-

Dienste für Inhalte mit hohem Schutzbedarf zu nutzen (VERTRAULICHE oder GEHEIME oder besonderen Geheimhaltungspflichten unterstehende Informationen, sowie besonders schützenswerte Personendaten).

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 in Ziff. 3.5 unten näher eingegangen wird.

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

Wo sind die Berner Daten in M365 genau?

Der Ort von Datenbearbeitungen ist gesetzlich geregelt: Gemäss Art. 14d des Datenschutzgesetzes (KDSG) 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 1 zur Datenschutzverordnung des Bundes[4] trifft das auf die EU- und EWR-Staaten zu, nicht aber auf die USA. Zudem schreibt Art. 10 Abs. 2 des Gesetzes über die digitale Verwaltung (DVG; BSG 109.1) vor, dass Daten nicht im Ausland aufbewahrt werden dürfen, wenn es den Behörden nicht möglich ist, die Kontrolle darüber auszuüben, wer Daten einsehen oder verändern kann, die nicht allen Personen zugänglich sein sollen.

Aus diesen Gründen werden die Berner Daten in M365 in folgenden Ländern bearbeitet:

- Aufbewahrt (gespeichert) und hauptsächlich bearbeitet werden die Berner Daten in einem Rechenzentrum von Microsoft in der Schweiz.
- Die Daten können auch in anderen Ländern der EU oder des EWR bearbeitet werden, etwa wenn das Schweizer Rechenzentrum ausfällt, 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. Dazu gehören nach dem Wissensstand des KAIO im März 2023 folgende:

- **Der Bund** plant einen hybriden Einsatz von M365, wie im Kanton Bern vorgesehen (s. oben): Sensitive Informationen werden lokal bearbeitet, andere in der Cloud. Am 15. Februar 2023 hat der Bundesrat der Nutzung von M365 in diesem Sinne zugestimmt.[5]

- **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.[6]

[4] Medienmitteilung des Bundesrates vom 31. August 2022
[5] «Bund führt Microsoft 365 ein», Medienmitteilung des Bundesrates vom 15. Februar 2023
[6] Dies ergibt sich aus Auskünften der Verwaltungen sowie 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 erarbeitet eine Risikoanalyse mit ähnlichen Anforderungen wie der

- **Im Kanton Bern** sind namentlich die Universität Bern und das Inselspital daran, M365 einzuführen. Auf Gemeindeebene hat der Gemeinderat der Stadt Bern am 5. April 2023 die Einführung von M365 genehmigt und die damit verbundenen Restrisiken akzeptiert.[7]

3. Risiken, Massnahmen, Restrisiken

Dieser Abschnitt stellt die wesentlichen ISDS-Risiken der Nutzung von M365 vor, ebenso wie die wesentlichen Massnahmen, die das KAIO ergreift, 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 Kantonsverwaltung.

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 in 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 sich 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 Art. 28 DVG in Anlehnung an das Bundesdatenschutzrecht Regeln für die Auftragsdatenbearbeitung durch Behörden vor: Sie ist nur zulässig, wenn die Daten so bearbeitet werden, wie die für den Datenschutz verantwortliche Behörde selbst es tun dürfte, wenn keine gesetzliche oder vertragliche Geheimhaltungspflicht die Beauftragung verbietet, und wenn die Auftragsbearbeiterinnen und -bearbeiter die Datensicherheit gewährleisten. Dies gibt den Massstab für die zu ergreifenden Massnahmen vor.

Kanton Bern, und setzt M365 in den Schulen ein. FR bietet dem Staatspersonal M365-Kurse an. GL hat M365 an den Schulen eingeführt (Tätigkeitsbericht 2020, S. 38). LU setzt M365 in den Schulen ein. In NW hat der Regierungsrat 2020 die Einführung von M365 beschlossen (RRB 486/2020, S. 2). OW setzt M365 in den Schulen ein. In SH stimmte der Stadt- und Regierungsrat am 25. Januar 2022 der Einführung von M365 zu (SRB 56/RRB 3/55). SO führt M365 mit dem neuen Arbeitsplatz «SO!Workplace» ein (RRB Nr. 2022/1335, S. 11). SG erteilte im März 2023 einen Zuschlag für die Integration von M365 in der Kantonsverwaltung (Amtsblatt vom 07.03.2023). TG rechnet «mit dem Einsatz von M365 im grossen Stil ab 2024» (Finanzplan 2024–2026, S. 18). In UR erfolgt der «Rollout von Windows 11 und Office 365» ab Dezember 2022 («Schwerpunkte der Finanzdirektion», S. 14). VD nutzt M365 als Plattform «Eduvaud» für schulische Zwecke. VS nutzt M365 ebenfalls für schulische Zwecke. In ZG beschloss der Regierungsrat im März 2023 den Einsatz von Teams (Medienmitteilung vom 31.03.2023). In ZH beschloss der Regierungsrat im März 2022 die Zulassung von M365 in der Kantonsverwaltung (RRB 2022-0542).

[7] GRB Nr. 2023-391 vom 05.04.2023; die in dem Beschluss genannten Restrisiken sind: «den möglichen Zugriff von US-Behörden auf in der Microsoft-Cloud gespeicherte Daten gestützt auf den sog. «Cloud Act»; die mangelnde Transparenz bei der Datenbearbeitung durch Unterbeauftragte der Microsoft; die Auftragsdatenbearbeitung durch Microsoft und in diesem Zusammenhang die (Rest-) Risiken einer Verletzung der Zweckbindung der Datenbearbeitung und des Zugriffs von Microsoft auf verschlüsselte «Kundendaten»; die Speicherung von Daten auf Servern ausserhalb der Schweiz bzw. der EU; die mangelnde Verfügbarkeit der Daten; das Weiterbestehen von Daten trotz Löschung; das Abhängigkeitsverhältnis zu Microsoft.»

Microsoft ist (mit wenigen Ausnahmen, s. unten) technisch in der Lage, die von Berner Behörden 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 Collaboration-Dienstleistungen erbringen kann, also es ermöglichen kann, dass Daten und Gespräche team- und organisationsintern geteilt werden.

Das Programm work@BE hat Lösungsansätze geprüft, bei denen die kantonalen Daten auch gegenüber Microsoft verschlüsselt bleiben, oder zumindest die Benutzernamen pseudonymisiert werden. Eine Analyse des KAIO führte aber dazu, diese Option zu verwerfen.[8] Solche Lösungen sind noch kaum praxiserprobt und sind 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 kantonalen 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 Berner Behörden nicht neu. Bereits heute haben die Auftragsdatenbearbeiter des Kantons, wie der Rechenzentrumsbetreiber Bedag, der Telefoniedienstleister Swisscom und der Netzwerkdiensteanbieter SPIE ICS, einen vergleichbaren Zugriff auf die von ihnen mit bearbeiteten Daten der Kantonsverwaltung. Bei der Nutzung von M365 ergibt sich jedoch ein höheres Risiko daraus, dass Microsoft nicht eine kantonseigene (wie Bedag) oder eine Schweizer staatlich beherrschte Unternehmung (wie Swisscom) ist, sondern eine US-amerikanische Privatunternehmung. Dies reduziert das Mass an Vertrauen, das ihr aus Berner Sicht entgegengebracht werden kann, und wohl auch die Wirksamkeit allfälliger rechtlicher Schritte zur Durchsetzung von Berner Interessen. Allerdings ist das Risiko insoweit mit demjenigen vergleichbar, das der Kanton bereits heute dadurch eingeht, dass er sein Netzwerk BE-Net durch die einem französischen Konzern zugehörige SPIE ICS betreiben lässt, oder dadurch, dass er das Polizeifunknetzwerk POLYCOM u.a. durch die chinesische Unternehmung Huawei warten lässt. Zudem haben bei Telefongesprächen und Videokonferenzen, an denen Personen ausserhalb der Kantonsverwaltung beteiligt sind, auch deren Fernmeldediensteanbieter Zugang zu den Gesprächsinhalten.

3.1.1 Massnahmen

Technische Massnahmen:

- Die M365-Software verfügt über Funktionen zum Klassifizieren von Dokumenten durch die Nutzenden. Sie erlaubt es, Auswertungen über die Bearbeitung klassifizierter Dokumente zu erzeugen, so dass die Vorgesetzten Verstösse gegen die Vorschriften über den Umgang mit klassifizierten Dokumenten erkennen und ahnden können.

- 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) 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 beim KAIO einen kostenpflichtigen Zusatzdienst, der E2EE für Videokonferenzen mit mehreren Teilnehmenden unterstützt, bestellen.

[8] Bericht «Ergebnisse aus dem PoC zur Verschlüsselung von Daten mit Eperi», KAIO, 5. Dezember 2022, Dok. #392580 V. 1.0 (Interner Bericht)

Organisatorische Massnahmen:

- Wie bereits erwähnt (Ziff. 2.3), verbietet das KAIO den Nutzenden per Weisung, M365-Cloud-Dienste für Inhalte mit hohem Schutzbedarf zu nutzen (ausser wenn E2EE genutzt wird, siehe oben). 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 (s. Ziff. 3.4 unten).
- Wie ebenfalls erwähnt, nutzt der Kanton Bern die M365-Services nur für Collaboration-Zwecke (Telefon, Video, Chat, Dateiaustausch), nicht aber für die Bearbeitung der grossen Datensammlungen der Konzern- und Fachapplikationen, für die elektronische Geschäftsverwaltung oder für E-Mail.
- Die Mitarbeitenden werden bei der Einführung von M365 bzw. des neuen BE-KWP in der ISDS-konformen Nutzung der neuen Services geschult.

Rechtliche Massnahmen:

- Die allgemeinen Geschäftsbedingungen (AGB) von Microsoft bzw. ihr *Data Protection Addendum* (DPA) und eine Zusatzvereinbarung, die Microsoft für die Schweizer Behörden mit der Schweizerischen Informatikkonferenz (SIK) abgeschlossen hat, verpflichten Microsoft stark zusammengefasst zur sicheren, vertraulichen und zweckgebundenen Bearbeitung aller Daten des Kantons Bern 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 kantonalen Daten der Benutzerverwaltung, der Ablagen zum Dateiaustausch, der Chats und (soweit nicht E2EE aktiviert ist) der Telefongespräche und Videokonferenzen der Nutzerinnen und Nutzer zuzugreifen. Diese dürfen weisungsgemäss nur Inhalte mit geringem Schutzbedarf enthalten, jedoch ist es wahrscheinlich, dass diese Weisung nicht immer eingehalten wird.

3.2 Kontrollverlust gegenüber ausländischen Behörden

Sobald Daten des Kantons 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)[9] 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.[10]

- Der CLOUD Act[11] erlaubt es US-Strafbehörden, mit richterlicher Genehmigung strafprozessual relevante Informationen von US-Unternehmen einzuverlangen, auch wenn diese ausserhalb der USA aufbewahrt werden.[12] Auf diesem Weg könnte Microsoft zur Herausgabe von Berner Kundendaten in einem Schweizer Rechenzentrum von Microsoft verpflichtet werden.

[9] Kodifiziert in 50 U.S.C. § 1801 ff.
[10] 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.
[11] Kodifiziert in 18 U.S.C. § 2523 ff.
[12] Vgl. im Einzelnen 18 U.S.C. § 2703.

Die Berner Kantonsverwaltung 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 erhalten.[13] 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 Rosenthal[14] typischerweise sehr tiefe Eintretenswahrscheinlichkeiten ausweist.

3.2.1 Massnahmen

Organisatorische Massnahmen:

- Einschränkung der Nutzung von M365 auf Inhalte mit geringem Schutzbedarf (s. Ziff. 3.1.1 oben).
- 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. Diese gilt aus der Sicht der Datenschutzbehörden als datenschutzrechtlich sicher (Art. 14a Abs. 1 KDSG). 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, s. Ziff. 2.3 oben am Ende).[15]

Rechtliche Massnahmen:

- Microsoft verpflichtet sich vertraglich, 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,[16] behördliche Anfragen wenn möglich gerichtlich anzufechten, und die betroffenen Personen unter bestimmten Umständen zu entschädigen.[17]

3.2.2 Restrisiken

Es ist möglich, dass in voraussichtlich sehr seltenen Einzelfällen kantonale Informationen in M365 durch US-Strafverfolgungsbehörden oder Nachrichtendienste eingesehen werden. In M365 dürfen weisungsgemäss nur Informationen mit geringem Schutzbedarf bearbeitet werden, jedoch ist es wahrscheinlich, dass diese Weisung nicht immer eingehalten wird (s. Ziff. 3.4 unten).

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 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 bearbeiten, nämlich «Abrechnungs- und

[13] 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 Herausgabeaufforderungen erhalten (einschliesslich von Schweizer Behörden), wobei allerdings in keinem Fall tatsächlich Kundeninhalte 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).
[14] Cloud-Compliance- und Risk-Assessment für den öffentlichen Sektor in der Schweiz (CCRA-PS), https://www.rosenthal.ch/downloads/Rosenthal_CCRA-PS.xlsx
[15] "Microsoft announces the phased rollout of the EU Data Boundary for the Microsoft Cloud begins January 1, 2023", Microsoft EU Policy Blog, 15. Dezember 2022
[16] DPA vom Januar 2023, S. 7, Abschnitt «Offenlegung verarbeiteter Daten»
[17] DPA vom Januar 2023, Anhang C

Kontoverwaltung», «Vergütung, «Interne Berichterstattung und Geschäftsmodellierung» und «Finanzberichterstattung».

Welche solcher Daten Microsoft genau erhebt, und wie sie sie bearbeitet, legt sie gegenüber der Kundschaft nicht vollständig offen. Daraus ergibt sich das Risiko, dass von der Kantonsverwaltung bearbeitete Personendaten zweckwidrig für eigene Zwecke von Microsoft bearbeitet werden können, und dass die Kantonsverwaltung 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 der Berner Datenschutz- und Personalgesetzgebung (z.B. Art. 12a ff. PG; BSG 153.01) und der Randdatenverordnung (RDV; BSG 153.011.5) erfolgt.

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

Der Kanton weiss nicht, wie genau Microsoft welche Rand- und Telemetriedaten über die Nutzung der M365-Services durch Angestellte des Kantons 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

Wie oben mehrfach erwähnt, verbietet das KAIO den Nutzenden per Weisung, M365-Cloud-Dienste für Inhalte mit hohem Schutzbedarf zu nutzen (ausser wenn E2EE genutzt wird). Damit beschränken sich die oben erwähnten Risiken grundsätzlich auf Informationen mit geringem Schutzbedarf.

Die rechtliche Verbindlichkeit dieser Weisung ergibt sich aus der Zuständigkeit des KAIO zum Erlass von Weisungen zur Nutzung der von ihm vermittelten Leistungen (Art. 11d Abs. 3 OrV FIN [BSG 152.221.171], gestützt auf Art. 21 Abs. 2 Bst. b DVG). Diese Weisung wird das KAIO den Nutzenden in geeigneter Form vermitteln. Sie ist für alle Nutzerinnen und Nutzer des BE-KWP verbindlich, einschliesslich der Mitglieder der Justizbehörden, der Aufsichtsbehörden und des Grossen Rates (Art. 4 Abs. 2 i.V.m. Art. 32 Abs. 1 Bst. a DVG).

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

- Die Nutzenden kennen die Weisung (noch) nicht, etwa im Fall neuer oder externer Mitarbeitenden.
- Die Nutzenden kennen die Klassifizierungsvorschriften (noch) nicht, zumal diese erst im Rahmen der Informationssicherheitsgesetzgebung, die zurzeit im Projekt IS@BE erarbeitet wird, verwaltungsweit eingeführt werden.
- Die Nutzenden ignorieren die Weisung bewusst, etwa weil es aufwändiger oder zeitraubender wäre, Daten ausserhalb von M365 auszutauschen oder zusammenzuarbeiten.

[18] Products and Services DPA (Stand Januar 2023), S. 8

3.4.1 Massnahmen

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

Technische Massnahmen:
- M365 erlaubt das Hochladen von Dokumenten in die Cloud nur, wenn sie in Bezug auf ihren Schutzbedarf klassifiziert wurden. Es wird so konfiguriert, dass es das Hochladen von als zu schützenswert klassifizierten Dokumenten unterbindet.
- Das KAIO prüft, inwieweit es ohne Verletzung der Vertraulichkeit von Informationen möglich ist, automatisch festzustellen, ob weisungswidrig als klassifiziert markierte Informationen in M365 bearbeitet werden, und diesfalls die Verantwortlichen automatisch über diese Verletzung der Sicherheitsvorschriften zu informieren.

3.4.2 Restrisiken

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

3.5 Rasche Änderungen der Services durch Microsoft

Grossen Hyperscaler 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 Folgekosten auslösen kann.

Für diesen Bericht ist vor allem relevant, dass neue Funktionen mit neuen ISDS-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 Techno-

logiekonzerne 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 ihr basierende Wirtschafts- und Gesellschaftsordnung fundamental verändern wird. Zu den experimentellen oder schon kommerziell verfügbaren Anwendungen gehören:

- Übersetzungen (wie DeepL, vom Kanton bereits eingesetzt)
- 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 beabsichtigt, unter dem Titel «Copilot» zukünftig Funktionen der generativen KI in ihre Produkte zu integrieren, mit denen z.B. Zusammenfassungen von Dokumenten oder Sitzungsprotokolle automatisch erstellt werden können sollen.[19] Solche Funktionen und ihre allfällige Nutzung durch die Kantonsverwaltung können ISDS-Risiken nach sich ziehen:

- Es wäre sicherzustellen, dass die KI-Bearbeitung der Berner Daten in einem datenschutzrechtlich sicheren Land erfolgt (Art. 14a KDSG).
- Wenn die KI-Systeme Berner Daten zum Training ihrer Computermodelle verwenden, könnte dies den Grundsatz der Zweckbindung von Personendaten verletzen, und durch das Einfliessen in die Modelle könnten die Berner 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 tönen, aber inhaltlich falsch sein (sog. «Halluzination»), was die Benutzenden oft nicht erkennen können.

Daher wird das Projekt work@BE, sobald Microsoft generative KI-Funktionen in M365 einführt, deren Nutzung durch Einstellungen deaktivieren (was gemäss Auskunft von Microsoft möglich sein wird) oder im Übrigen durch Weisung verbieten, bis die Funktionen auf ihre Risiken hin geprüft wurden und geeignete Massnahmen zur Behandlung der Risiken bestimmt sind.

Umgekehrt ist es auch möglich, dass neue Funktionen dazu beitragen, dass bestehende ISDS-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:

- Das Programm work@BE und später im Betrieb das Service Management BE-KWP beobachten die Veränderungen von M365 laufend und beurteilen sie zusammen mit den Rechts-, Sicherheits- und Datenschutzverantwortlichen auf mögliche neue Risiken. Sie beobachten dazu neben der Dokumentation von Microsoft auch weitere relevante Quellen wie die Erkenntnisse von Datenschutzbehörden weltweit oder Medienberichte.
- Bei datenschutzrechtlich wesentlichen Änderungen wird das KAIO die DSA erneut mit einer Vorabkontrolle befassen und nötigenfalls dem Regierungsrat eine angepasste Liste von Restrisiken zum Akzept vorlegen.

[19] S. z.B.: "Introducing Microsoft 365 Copilot – your copilot for work", Official Microsoft Blog, 16. März 2023

- Für den Fall, dass die weitere Nutzung von M365 aufgrund neuer Risiken als zu riskant beurteilt wird, bereitet das KAIO eine Exit-Strategie vor (s. Ziff. 3.8.1 unten).

Rechtliche Massnahmen:

- Für den Fall, dass die weitere Nutzung von M365 aufgrund neuer Risiken als zu riskant beurteilt wird, kann der Kanton Bern den Vertrag über die Nutzung von M365 relativ kurzfristig (längstens innerhalb eines Jahres) kündigen.

3.5.2 Restrisiken

Es ist möglich, dass neue ISDS-Risiken, die sich zukünftig möglicherweise aus neuen Funktionen von M365 ergeben, nicht bzw. spät erkannt werden, oder, dass diese Risiken sich als nicht mitigierbar 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 (was für den Kanton Bern nicht der Fall ist):

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 ISDS-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 Programms work@BE ergab, dass die zurzeit ausgewiesenen Subunternehmen (Stand der Liste: 6. Februar 2023), soweit sie für Leistungen an den Kanton Bern überhaupt zum Einsatz gelangen, keine unakzeptablen ISDS-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 ISDS-Risiken verbunden sind. In diesem Fall hat der Kanton Bern kein Recht, den Einsatz solcher Subunternehmen abzulehnen, sondern kann lediglich mit verkürzter Frist den Vertrag mit Microsoft kündigen.

3.6.1 Massnahmen

Organisatorische Massnahmen:

- Das KAIO beobachtet im Rahmen der laufenden Überwachung der Weiterentwicklung von M365 (s. Ziff. 3.5.1 oben) auch allfällige Anpassungen der Subunternehmenliste und beurteilt die sich daraus ergebenden Risiken. Es geht mit ihnen wie in Ziff. 3.5.1 oben beschrieben um.

Rechtliche Massnahmen:

- Für den Fall, dass die weitere Nutzung von M365 aufgrund neuer Subunternehmen als zu riskant beurteilt wird, kann der Kanton Bern den Vertrag über die Nutzung von M365 kurzfristig (innerhalb von sechs Monaten) kündigen.

3.6.2 Restrisiken

Es ist möglich, dass Microsoft dereinst Subunternehmen beizieht, die aus der Sicht des Kantons ein ISDS-Risiko darstellen. In diesem Fall kann der Kanton diese Subunternehmen nicht ablehnen, sondern nur den Vertrag kündigen.

3.7 Begrenzte Überprüfbarkeit der Umsetzung der vertraglichen Massnahmen

Microsoft verpflichtet sich zwar, wie oben ausgeführt, vertraglich zur Umsetzung von weitgehenden ISDS-Massnahmen. Für den Kanton Bern ist die Art und Weise, wie Microsoft ihre Leistungen erbringt,

[20] Vgl. allgemein Microsoft Trust Center, Microsoft Data Access Management, abgerufen 3. Juni 2023

aber nicht transparent; er kann nicht «hinter die Kulissen» der Rechenzentren und der Softwareentwicklung von Microsoft blicken. Damit kann er in den meisten Fällen nicht selbst überprüfen, ob Microsoft ihre ISDS-Verpflichtungen einhält.

Auch dieses Risiko ist bis zu einem bestimmten Grad allen Auftragsdatenbearbeitungen inhärent, so auch den bereits erwähnten bestehenden Auftragsdatenbearbeitungen des Kantons durch Unternehmen wie Bedag, Swisscom oder SPIE ICS. Wie bei diesen bestehenden 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 Auditberichten.[21] Im Vergleich zum kantonalen 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 der Kanton mit M365 einen Service nutzt, der von Millionen Menschen und Hunderttausenden Unternehmen und Behörden weltweit genutzt wird, kann sich zur Überprüfung der Umsetzung der vertraglichen Massnahmen aber als Vorteil auswirken: Der Kanton ist nicht darauf angewiesen, alle möglichen Umsetzungsdefizite selbst erkennen und nachweisen zu müssen. Vielmehr kann er die Synergien nutzen, die sich daraus ergeben, dass die globalen Fachmedien, viele Datenschutzaufsichtsbehörden und viele andere Kunden mit ähnlichen oder höheren Sicherheits- und Datenschutzanforderungen die Leistungserbringung durch Microsoft ebenfalls aktiv im Auge behalten.

3.7.1 Massnahmen

Organisatorische Massnahmen:
- Das KAIO beobachtet im Rahmen der laufenden Überwachung der Weiterentwicklung von M365 (s. Ziff. 3.5.1 oben) 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 KAIO mit anderen Grosskunden von M365, primär anderen Schweizer öffentlichen Verwaltungen 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 Microsoft bestehen, prüft das KAIO die Ausübung des vertraglichen Auditrechts im Verbund mit anderen M365-Grosskunden.
- Wenn Vertragsverletzungen festgestellt sind und anhalten, prüft das KAIO 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 ISDS-Verpflichtungen verletzt, ohne dass der Kanton das (zeitnah) weiss.

[21] DPA vom 1. Januar 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 der Kanton bereits in einem solchen Abhängigkeitsverhältnis zu seinen wichtigen Softwarelieferanten wie SAP 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 kantonalen Verwaltungsabläufe integriert, als dies bei den bisherigen Lösungen wie Skype und Sharepoint der Fall war.

Gleichzeitig muss der Kanton 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. Dies können zu hohe Preise, gewichtige Sicherheits- oder Datenschutzdefizite, oder geänderte rechtliche und politische Rahmenbedingungen gehören.

3.8.1 Massnahmen

Organisatorische Massnahmen:

- Das Projekt work@BE erarbeitet einen Ausstiegsplan (Exit-Strategie), die aufzeigt, wie in dem Fall, dass der Kanton M365 nicht mehr nutzen will, kann oder darf, rasch eine Alternativlösung evaluiert und eingeführt wird. Die Exit-Strategie umfasst das laufende Backup aller Dokumente bei der Bedag und die Identifikation von Alternativen zu M365. Dies wird in die bereits bestehenden, vertraglich geregelten Betriebsprozesse von Bedag integriert.

3.8.2 Restrisiken

Für den Fall, dass der Kanton 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.