Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei
Amtbis
Digitale Transformation und IKT-Lenkung (DTI)

NICHT KLASSIFIZIERT

Cloud Enabling Büroautomation (CEBA)

Rechtsgrundlagenanalyse für den Einsatz von Microsoft (M365)

Projektauftraggeber	Marc Lussi
Projektleitung	Brigitte Gerber
Autorin	Marc Unternährer, Sandro Aebischer
Status	Abgeschlossen

Bern, 10.07.2025

Inhaltsverzeichnis

1 Ausgangslage 3
2 Bestehende Rechtsgrundlagen 3
2.1 Legalitätsprinzip 3
2.2 Zentral bereitgestellte IKT-Mittel 3
2.3 Informationssicherheit 4
2.3.1 Auswirkungen des ISG für M365 4
2.3.2 Sicherheit beim Einsatz von Informatikmitteln 5
2.3.3 Schutzbedarf für Informationen 6
2.4 Datenschutz 6
2.4.1 Auftragsdatenbearbeitung 7

2.4.2 Datenbekanntgabe ins Ausland 7
2.4.3 US-CLOUD Act 8
2.4.4 Gever-Verordnung 8
2.4.5 Randdatenverordnung 8
2.4.6 Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste 9
2.4.7 Abhören und Aufnehmen fremder Gespräche 9
2.5 Amtsgeheimnis 9
3 Schlussfolgerung und Empfehlung 10

1 Ausgangslage

Die Firma Microsoft verfolgt die Strategie «Cloud first». Die Weiterentwicklung neuer Office- und Kollaborations-Funktionen erfolgt nur noch in der Public Cloud. Die aktuell bei der Bundesverwaltung eingesetzte Office-Version muss ersetzt werden, weil wichtige Office-Anwendungen ans Ende ihres Lebenszyklus gelangt sind und vom Hersteller Microsoft in absehbarer Zeit nicht mehr unterstützt werden.

Mit dem Projekt Cloud Enabling Büroautomation (CEBA) wird Microsoft 365 (M365) als neuer Standard in der zentralen Bundesverwaltung voraussichtlich bis Ende 2025 eingeführt.

Mittel- bis langfristig können viele bestehende oder neue Funktionen nicht mehr aus dem eigenen Rechenzentrum (On-Premises) bereitgestellt werden. Jedoch bleibt es mit M365 möglich, Dokumente lokal auf dem Endgerät zu bearbeiten und im eigenen Rechenzentrum zu speichern.

Das vorliegende Dokument liefert eine grobe Übersicht über die bestehenden Rechtsgrundlagen für deine Cloud-Nutzung der Bundesverwaltung. Für eine vertiefte Auseinandersetzung zu einzelnen rechtlichen Aspekten der Cloud-Nutzung kann auf den von der Bundekanzlei publizierten Bericht «Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung» vom März 2025 verwiesen werden.[1]

2 Bestehende Rechtsgrundlagen

2.1 Legalitätsprinzip

Gemäss dem in Artikel 5 Absatz 2 BV (SR 101) festgehaltenen Legalitätsprinzip setzt jede staatliche Tätigkeit eine gesetzliche Grundlage voraus.

Die Nutzung von M365 im Rahmen der Büroautomation ist als administrative Hilfstätigkeit (oder Bedarfsverwaltung) zu qualifizieren. Darunter sind Tätigkeiten zu verstehen, die nicht direkt die Wahrnehmung einer Staatsaufgabe darstellen, die es aber braucht, um eine bestimmte Staatsaufgabe zu erfüllen. Dazu gehören auch die Beschaffung und der Unterhalt der elektronischen Infrastruktur, die für die Erfüllung bestimmter Aufgaben notwendig ist. Für administrative Hilfstätigkeiten sind die Anforderungen des Legalitätsprinzips weniger streng; sie benötigen keine spezifische gesetzliche Grundlage.

Die gesetzliche Grundlage für die administrative Hilfstätigkeit leitet sich aus der Rechtsgrundlage der jeweiligen öffentlichen Aufgabe ab. Mit der Begründung einer Aufgabe wird auch die Kompetenz verliehen, die dafür erforderlichen Mittel zu beschaffen. Je nach Sachbereich oder Art der bearbeiteten Daten gelten aber noch spezifischere Anforderungen an die Rechtsgrundlage. Das gilt namentlich dann, wenn Personendaten oder geschützte Informationen betroffen sind.

2.2 Zentral bereitgestellte IKT-Mittel

Gemäss Artikel 11 Absatz 1 des Bundesgesetzes über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBAG; SR 172.019) sowie Artikel 11 Absatz 1 der Digitalisierungsverordnung (DigiV; SR 172.019.1) kann der Bereich DTI die zentrale Bereitstellung eines IKT-Mittels und damit zusammenhängende Dienstleistungen anordnen bzw. selbst zentral bereitstellen und zudem nach Artikel 40 Abs. 1 Bst. e DigiV Weisungen dazu erlassen.

Der IKT-Standarddienst Büroautomation (BA) umfasst den standardisierten Funktionsumfang der Büroautomation, Dienste des Unified Communication Collaboration (UCC), die Bereitstel-

[1] www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Bundesarchitektur > Cloud > Dokumente > Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung

lung von Druckerleistungen, die mit dem Bundesnetz verbundenen Smartdevices und die entsprechenden Infrastruktur-Services zur Büroautomation. Der Leistungsumfang wird in den Weisungen zur Steuerung und Führung der Standarddienste gemäss VDTI (W008) näher umschrieben. M365 ist Teil des Standarddienstes Büroautomation (BA) der vom Bereich DTI zentral bereitgestellt wird.

2.3 Informationssicherheit

Das Informationssicherheitsgesetz (ISG, SR 128) soll Informationen und Informatikmittel des Bundes schützen. Das ISG hat einen weiten institutionellen Geltungsbereich: Es gilt für alle Bundesbehörden (Parlament, Bundesrat, eidgenössische Gerichte, Bundesanwaltschaft und ihre Aufsichtsbehörde und Nationalbank; sog. Verpflichtete Behörden nach Art. 2 Abs. 1 ISG) und ihre unterstellten Organisationen (insb. Departemente, Bundeskanzlei, zentrale und dezentrale Verwaltungseinheiten, samt Armee; sog. verpflichtete Organisationen nach Art. 2 Abs. 2 ISG). Externe öffentlich-rechtliche oder private Organisationen, die mit Bundesaufgaben betraut werden, gelten ebenfalls als verpflichtete Organisationen und sind in Bezug auf ihre Verwaltungsaufgaben dem ISG unterstellt. Der Bundesrat hat jedoch auf dem Verordnungsweg Organisationen der dezentralen Bundesverwaltung sowie verwaltungsexterne Organisationen des öffentlichen oder privaten Rechts, die mit Verwaltungsaufgaben betraut sind, vom Geltungsbereich des ISG ausgenommen, soweit sie nicht klassifizierte Informationen des Bundes bearbeiten, auf Informatikmittel des Bundes zugreifen oder solche betreiben lassen (Art. 2 Abs. 2 Informationssicherheitsverordnung [ISV; SR 128.1]). Dritte, welche nicht unter den Geltungsbereich des ISG fallen, sind mit vertraglichen Vereinbarungen zur Einhaltung der Bestimmungen nach ISG zu verpflichten (vgl. Art. 9 ISG) bzw. gegebenenfalls dem Betriebssicherheitsverfahren zu unterziehen (Art. 49 ff. ISG).

Mit den Einsatzrichtlinien UCC (E017) und Microsoft 365 (E031)[2] hat der Bereich DTI unter anderem gewisse informationssicherheitsrechtliche Aspekte von M365 umgesetzt.

2.3.1 Auswirkungen des ISG für M365

Die sichere Bearbeitung aller Informationen und Informatikmittel, für die der Bund zuständig ist (auch die nicht-klassifizierten Informationen), muss gewährleistet sein. Die zuständigen Stellen sorgen gemäss Artikel 6 Absatz 2 ISG insbesondere dafür, dass die Informationen ihrem Schutzbedarf entsprechend:

- nur Berechtigten zugänglich sind (Vertraulichkeit);
- verfügbar sind, wenn sie benötigt werden (Verfügbarkeit);
- nicht unberechtigt oder unbeabsichtigt verändert werden (Integrität);
- nachvollziehbar bearbeitet werden (Nachvollziehbarkeit).

Die Massnahmen zur Sicherheit der Informatikmittel sollen jedoch stets zweckmässig und wirtschaftlich sinnvoll sein. Es ist eine Kosten-Nutzenabwägung vorzunehmen.[3]

Gemäss der Legaldefinition nach Artikel 5 Buchstabe a ISG werden als Informatikmittel «Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen» bezeichnet. Alle Informationen, die im Rahmen des Projekts CEBA in Hybrid-Cloud-Umgebungen ausgelagert werden, fallen somit in den Anwendungsbereich des ISG und der ISV. Die Bestimmungen des ISG und des ISV gelten zwar

[2] www.bk.admin.ch > Digitale Transformation und IKT-Lenkung > Standarddienste > Büroautomation > Projekt CEBA > Dokumente > E031 – Einsatzrichtlinie Microsoft 365

[3] Siehe dazu Botschaft ISG, BBl 2017 2953, 3012.

nicht für Microsoft. Beim Einsatz von Cloud-Anbietern müssen aber die erforderlichen Massnahmen der Informationssicherheit vertraglich (vgl. Art. 9 ISG) geregelt werden.

Das ISG regelt zwei Faktoren, die für den Einsatz einer Cloud-Lösung in seinem Geltungsbereich massgebend sind: Erstens die darin zu bearbeitenden Informationen (klassifizierte vs. nicht-klassifizierte Information) und zweitens das Resultat des Sicherheitsverfahrens bzw. ob ein Informatikmittel der Sicherheitsstufe «Grundschutz», «hoher Schutz» oder «sehr hoher Schutz» gemäss Artikel 17 ISG zuzuordnen ist.

Insbesondere müssen folgende Punkte geprüft werden:

- Die *Informatikmittel* wie M365 müssen innerhalb von zwei Jahren nach Inkraftsetzung des ISG und somit bis 31. Dezember 2025 nach den neuen Bestimmungen des ISG eingestuft werden (Art. 90 Abs. 2 ISG);
- *Personensicherheitsprüfungen (PSP)*: Nach bisherigem Recht ausgestellte Sicherheits- und Risikoerklärungen sind fünf Jahre ab deren Ausstellung gültig. Hinsichtlich bestehender Prüfungen muss nichts unternommen werden. Für neue Mitarbeitende erfolgt die PSP nach den Bestimmungen des ISG;
- *Betriebssicherheitsverfahren (BSV): Nach altem Recht ausgestellte Betriebssicher*heitserklärungen (BSE) sind fünf Jahre ab deren Ausstellung gültig. Die Projektleitung muss bei sicherheitsempfindlichen Aufträgen sicherstellen, dass der Anbieter über eine gültige BSE verfügt, ggf. unter Hinzuziehung der Fachstelle Betriebssicherheitsverfahren (vgl. Verfahren nach der Verordnung über die Personensicherheitsprüfungen [VBSV; SR 128.31). Wenn noch keine BSE ausgestellt wurde, ist eine entsprechende zu besorgen bzw. dies wäre beispielsweise aufgrund des in der Schutzbedarfsanalyse (vgl. Ausführungen in Ziff. 2.3.2 nachstehend) ausgewiesenen Schutzbedarfs zu prüfen (vgl. Verfahren nach der VBSV.

2.3.2 Sicherheit beim Einsatz von Informatikmitteln

Zur Gewährleistung der Informationssicherheit beim Einsatz von Informatikmitteln muss gemäss Artikel 16 Absatz 1 ISG ein Sicherheitsverfahren festgelegt werden. Das betrifft auch die Auslagerung von Daten und Informationen in eine Hybrid-Cloud-Umgebung. Neben den traditionellen IKT-Elementen (wie z.B. aktive Netzwerkkomponenten, Server und andere Produkte der Informatik) sind auch «Services», «Informationssysteme» und namentlich «Datensammlungen» Teil des Sicherheitsverfahrens. Damit sind jegliche Datensammlungen auf die Konformität mit dem ISG und der ISV zu überprüfen, die in irgendeiner Form innerhalb der Bundesverwaltung generiert, gepflegt, outgesourced oder in anderer Form bearbeitet werden.

Ein Sicherheitsverfahren nach Artikel 16 ISG umfasst unter anderem die Beurteilung des Schutzbedarfs der Informationen vor dem Einsatz von Informatikmitteln (Art. 16 Abs. 2 Bst. a ISG). Dieses Verfahren wird summarisch als Schutzbedarfsanalyse (Schuban) bezeichnet und muss vor Projektfreigabe vorliegen und alle 5 Jahre überprüft werden (Art. 25 ISV). Zudem müssen Informatikmittel bis Ende 2025 aufgrund der neu geltenden Klassifizierung des ISG (Art. 90 ISG) neu eingestuft werden. Die Schuban hilft festzustellen, welche Daten vom Informatikmittel bearbeitet werden. Auf dieser Basis ist dann zu prüfen, welche Anforderungen erfüllt werden müssen. Artikel 16 Absatz 2 ISG regelt weiter die Umsetzung der Sicherheitsmassnahmen und deren Überprüfung (Bst. b), die Zuständigkeit für die Sicherheitsfreigabe des Informatikmittels (Bst. c) oder das Vorgehen bei Veränderung der Risiken (Bst. d).

In Bezug auf das Projekt CEBA bedeutet dies, dass die potenziellen Risiken eruiert werden müssen, bevor Daten in die Cloud ausgelagert werden können. Sollte sich aus der Schuban ein erhöhter Schutzbedarf ergeben müssen die Verwaltungseinheiten zusätzliche Sicherheitsmassnahmen prüfen und allfällige Restrisiken ausweisen (Art. 27 ISV).

2.3.3 Schutzbedarf für Informationen

Neben der Bestimmung der Sicherheitsstufe des Informatikmittels, können Informationen gemäss den drei Klassifizierungsstufen INTERN (Art. 18 ISV), VERTRAULICH (Art. 19 ISV) und GEHEIM (Art. 20 ISV) klassifiziert werden.

Gemäss den jeweils am 16. Juni 2024 in Kraft getretenen Einsatzrichtlinien UCC (E017) und Microsoft 365 (E031) ist eine Bearbeitung von klassifizierten Informationen in den cloudbasierten M365-Services grundsätzlich nicht zulässig.

Das heisst, nur *nicht klassifizierte Informationen* dürfen bearbeitet werden, sofern die Einsatzrichtlinien keine ausdrückliche Ausnahme vorsehen – insbesondere unter Anwendung der Ende-zu-Ende-Verschlüsselung. Beispielsweise dürfen während der Sprach- und/oder Videokommunikation (inkl. Desktopfreigabe) in MS Teams als INTERN klassifizierte Informationen entsprechend verschlüsselt ausgetauscht werden, wohingegen eine Transkription nicht möglich bzw. ein Austausch per Chat nicht zugelassen ist. Als VERTRAULICH klassifizierte Informationen dürfen nur im Rahmen lokal installierter Office Anwendungen und nur unter Schutz der freigegebenen Verschlüsselungsumgebung in M365 bearbeitet werden. Die Vorgaben und Einschränkungen für die Klassifikation INTERN werden nach Vorliegen der Bearbeitungsvorschriften vom SEPOS neu geprüft und bei Bedarf angepasst.

Der konkrete Verwendungsumfang hängt zudem von der Art des jeweiligen Endgeräts ab (vgl. Anhang A der Einsatzrichtlinie Microsoft 365 [E031]).

Bezüglich der Nutzung von generativer KI (vorliegend MS Copilot) hat die Bundesverwaltung mit dem Merkblatt zur Verwendung von generativen KI-Werkzeugen in der Bundesverwaltung vom 18. Januar 2024 eine entsprechende Umsetzung übergeordneter Vorgaben formuliert. Demnach ist es untersagt, als INTERN, VERTRAULICH oder GEHEIM klassifizierte Informationen in die Systeme einzugeben. Darüber hinaus dürfen auch Informationen, die zwar nicht klassifiziert sind, aber sensible Informationen enthalten (Amtsgeheimnisse, besondere [Berufs-] Geheimnisse, vertraglich ausdrücklich geschützte Informationen), nicht für Eingaben in KI-Systeme verwendet werden.

2.4 Datenschutz

Wenn Personendaten in die Cloud ausgelagert bzw. im Rahmen von Cloud basierten Services von M365 bearbeitet werden sollen, sind die Vorgaben der Datenschutzgesetzgebung einzuhalten. Unter *Bearbeiten* wird gemäss Artikel 5 Buchstabe d des Datenschutzgesetzes (DSG; SR 235.1) «jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, *insbesondere* das Beschaffen, Speichern, Aufbewahren, Verwenden, Verändern, Bekanntgeben, Archivieren, Löschen oder Vernichten von Daten» verstanden. Ein «Bearbeiten» ist auch das blosse Übermitteln von Daten an einen Cloud-Dienstleister.

Das DSG definiert neben den Personendaten Kategorien von Daten, bei deren Bearbeitung zusätzlich strengere Anforderungen gelten: besonders schützenswerten Personendaten (Art. 5 Bst. c DSG). Für die Bearbeitung von Daten, die in diese Kategorien fallen, ist in der Regel eine Rechtsgrundlage in einem Bundesgesetz notwendig (Art. 34 Abs. 2 Bst. a DSG). Ebenfalls ein Gesetz im formellen Sinn ist im Falle eines Profilings (Art. 5 Bst. f DSG) erforderlich (Art. 34 Abs. 2 Bst. b DSG). Abweichungen von diesem Erfordernis sind zulässig, wenn der Bundesrat die Bearbeitung bewilligt hat, weil er die Rechte der betroffenen Personen für nicht gefährdet hält oder die betroffene Person im Einzelfall in die Bearbeitung eingewilligt hat (Art. 34 Abs.4 Bst. a und b DSG).

Gemäss den geltenden Einsatzrichtlinien UCC (E017) und Microsoft 365 (E031) ist zwar eine Bearbeitung von Personendaten, grundsätzlich nicht aber von besonders schützenswerten Personendaten in den cloudbasierten M365-Services zulässig.

Analog zu den Ausführungen zur Informationssicherheit in Ziffer 2.3.3 sehen vorgenannte Einsatzrichtlinien ausdrücklich Ausnahmen von diesem Grundsatz vor. Das heisst, unter Anwendung der Ende-zu-Ende-Verschlüsselung dürfen besonders schützenswerte Personendaten während der Sprach- und/oder Videokommunikation (inkl. Desktopfreigabe) in MS Teams bearbeitet werden. Nicht zulässig ist hingegen eine Bearbeitung im Rahmen der Transkriptions- sowie Chatfunktion.

In KI-Systeme dürfen aber keine Personendaten (jeglicher Art) eingegeben werden.[4]

2.4.1 Auftragsdatenbearbeitung

Bei der Bearbeitung von personenbezogenen Daten mit Cloud-Lösungen kann es sich um eine Auftragsdatenbearbeitung im Sinne der Datenschutzgesetzgebung handeln. Der Cloud-Service-Anbieter ist aber nicht in jedem Fall Auftragsdatenbearbeiter nach Art. 9 DSG. Die entsprechende Qualifikation hängt insbesondere auch vom gewählten Modell ab[5]. In der Regel wird der Cloudanbieter die Auftragsbearbeitung zumindest sehr beschränkt wahrnehmen, weil er nur in ganz bestimmten und im Voraus vereinbarten Einzelfällen auf die Daten zugreifen kann. Liegt eine Auftragsdatenbearbeitung vor, müssen die Anforderungen von Art. 9 DSG erfüllt werden.

Verantwortlich bleibt die Verwaltungseinheit, da sie im Rahmen der gesetzlichen Grundlage für die Bearbeitung entscheidet, wie bzw. mit welchen Mitteln die Daten bearbeitet werden (Art. 9 Abs. 2 DSG). Sie muss die Auftragsdatenbearbeiter sorgfältig auswählen, instruieren und kontrollieren und damit aktiv sicherstellen, dass diese die datenschutzrechtlichen Vorgaben so einhalten, wie sie es selbst tun müssten. Auch wenn Cloudanbieter nicht auf die Daten selbst zugreifen können, so sind sie vertraglich zur Gewährleistung der Einhaltung der datenschutzrechtlichen Anforderungen und der Datensicherheit zu verpflichten.

Artikel 12 DigiV regelt die Voraussetzungen, unter denen nicht allgemein zugängliche Daten externen Leistungserbringern zugänglich gemacht werden dürfen. Ein Zugänglichmachen ist nur zulässig, wenn zur Erbringung der Leistung erforderlich (Bst. a), die für die Daten verantwortliche Bundesbehörde zugestimmt hat (Bst. b) und angemessene vertragliche, organisatorische und technische Vorkehrungen getroffen wurden, um eine weitere Verbreitung der Daten zu verhindern (Bst. c).

2.4.2 Datenbekanntgabe ins Ausland

Bei einer Datenbekanntgabe ins Ausland (Art. 16 ff. DSG) muss zusätzlich ein angemessenes Schutzniveau erreicht werden. Personendaten dürfen ins Ausland bekannt gegeben werden, wenn der Bundesrat festgestellt hat, dass die Gesetzgebung des betreffenden Staates einen angemessenen Schutz gewährleistet (Art. 16 Abs. 1 DSG). Diese Staaten werden in einer Liste im Anhang 1 der Datenschutzverordnung (DSV; SR 235.11) aufgeführt. Aktuell erfüllen namentlich die Mitgliedstaaten der EU, UK, USA im Rahmen des Swiss-U.S. Data Privacy Frameworks, Argentinien und Neuseeland diese Anforderungen, im Gegensatz bspw. zu China.

Da es sich bei Microsoft ein ausländisches Unternehmen handelt, stell sich die Frage, ob durch die Nutzung von M365 eine Datenbekanntgabe ins Ausland im Sinne des DSG vorliegt. Dies ist z.B. dann grundsätzlich nicht der Fall, wenn Daten anonymisiert und verschlüsselt sind oder wenn andere Vorkehrungen getroffen werden, um eine Kenntnisnahme vom Dateninhalt bzw. «Klartext» durch den Cloud-Anbieter auszuschliessen.

Eine Datenbekanntgabe ins Ausland ist aber möglich und in einem solchen Fall ist der Cloud-

---

[4] vgl. Merkblatt zur Verwendung von generativen KI-Werkzeugen in der Bundesverwaltung vom 18. Januar 2024 www.cnai.swiss > Dienstleistungen > Weitere Dienstleistungen > Merkblätter zu KI in der Bundesverwaltung

[5] Vgl. Ziff. 1.5.1 Rechtlicher Rahmen für die Nutzung von Public-Cloud-Diensten in der Bundesverwaltung

Anbieter vertraglich zu verpflichten, sich generell an das schweizerische Recht und insbesondere an die datenschutzrechtlichen Vorgaben zu halten. Microsoft darf deshalb Daten nur in ausländischen Staaten mit angemessenen Datenschutzniveau gemäss DSV bearbeiten und speichern. Es muss offengelegt sein, wo der Cloud-Service effektiv betrieben wird (inkl. Supportleistungen), wer von wo aus auf die Daten Zugriff hat.

2.4.3 US-CLOUD Act

Da es sich bei Microsoft um eine Unternehmung mit Sitz in den USA handelt, stellt sich die Frage, ob aufgrund nachrichtendienstlicher Überwachungsprogramme oder dem US-CLOUD Act (Clarifying Lawful Overseas Use of Data Act) Zugriffe auf Daten des Bundes ermöglicht werden, ohne dass ein Rechtshilfeverfahren durchgeführt wird. Insbesondere der Foreign Intelligence Surveillance Act (FISA) und der CLOUD Act werden bisweilen als erhebliche Risiken wahrgenommen.

Datenzugriffe durch amerikanische Behörden sind somit zwar nicht ausgeschlossen, die Tragweite des Risikos dürfte indessen überschaubar sein. Grundsätzlich sind die behördlichen Massnahmen nach diesen Gesetzen an bestimmte Voraussetzungen gebunden. So können nur Strafverfolgungsbehörden zur Verfolgung schwerer Straftaten gestützt auf den CLOUD-Act vorgehen. Daten müssen von den erfassten Diensteanbietern auch nur dann herausgegeben werden, wenn sie darüber faktische oder rechtliche Kontrolle haben. Zudem bestehen verfahrensrechtliche Sicherungen; die Cloud-Anbieter können die Massnahmen anfechten[6]. Auskünfte werden in relativ wenigen Fällen erteilt, in der Regel bezüglich Metadaten, selten sind Inhaltsdaten Gegenstand[7].

Seit dem Inkrafttreten der Änderungen von Anhang 1 DSV am 15. September 2024 können Personendaten aus der Schweiz an im Rahmen des Swiss-U.S. Data Privacy Frameworks zertifizierte Organisationen in den USA ohne zusätzliche Garantien übermittelt werden. Die aktuellen politischen Entwicklungen in den USA werden durch die zuständigen Stellen beobachtet.

Um im Übrigen das Risiko eines Behördenzugriffs zu senken, kann mit geeigneten technischen Massnahmen verhindert werden, dass Microsoft Zugriff auf die Daten erhält. Dieser kann nicht zur Entschlüsselung von Daten gezwungen werden, wenn er nicht über die Schlüssel verfügt. Die Herausgabe von Inhaltsdaten in solchen Verfahren ist sehr selten.

2.4.4 Gever-Verordnung

Die Gever-Verordnung (SR 172.010.441) regelt die Bearbeitung von geschäftsrelevanten Informationen in elektronischen Geschäftsverwaltungssystemen durch die Bundesverwaltung. Die GEVER-Verordnung legt in Artikel 11 Absatz 1 fest, dass alle Informationen ab Stufe VERTRAULICH in den Geschäftsverwaltungssystemen verschlüsselt werden müssen. Da grundsätzlich nur nicht klassifizierte Daten in M365 bearbeitet werden dürfen (vgl. Ausführungen in 2.3.3 und 2.4 vorstehend), ist das unproblematisch.

2.4.5 Randdatenverordnung

Das Projekt CEBA umfasst unter anderem Daten der Mitarbeiter der Bundesverwaltung. Für die Bearbeitung dieser Daten besteht eine spezifische gesetzliche Grundlage in Bezug auf die Datenbearbeitung bei der Nutzung der elektronischen Infrastruktur innerhalb der Bundesverwaltung (Art. 57i ff. RVOG; SR 172.010). Die elektronische Infrastruktur umfasst sämtliche

[6] Vgl. Z.B. Neue Massnahmen zum Schutz Ihrer Daten – Microsoft Schweiz Newsroom;

[7] Vgl. z.B. Law Enforcement Request Report | Microsoft CSR;

stationären oder mobilen Anlagen und Geräte, die Personendaten und Daten juristischer Personen aufzeichnen können (Art. 57k RVOG). Artikel 57j Absatz 1 RVOG legt den Grundsatz fest, dass Verwaltungseinheiten Personendaten, die bei der Nutzung der elektronischen Infrastruktur anfallen, grundsätzlich nicht aufzeichnen oder auswerten dürfen.

Gestützt auf Artikel 57q Absatz 1 RVOG hat der Bundesrat in der sog. Randdatenverordnung (VBNIB; SR 172.010.442) die Zugriffsberechtigung, Aufbewahrungsdauer, Vernichtung sowie Auswertung dieser Personendaten geregelt. Bei der Aufbewahrungsdauer wird zwischen bewirtschafteten und nicht bewirtschafteten Daten unterschieden (Art. 4 f. VBNIB); letztere sind im Prinzip rasch zu vernichten. Verantwortlich für Aufbewahrung und Vernichtung der Personendaten sind die Betreiberin der elektronischen Infrastruktur (in der Regel das BIT) sowie das Bundesorgan, das für den Datenschutz zuständig ist bzw. die Geräte nutzt (Art. 6 VBNIB).

2.4.6 Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste

Die Identitäts- und Zugriffsverwaltung Bund (IAM Bund) sorgt dafür, dass die richtigen Personen und Anwendungen zum richtigen Zeitpunkt den richtigen Zugriff auf Ressourcen der Bundesverwaltung erhalten. Die Datenbearbeitung im Rahmen der Identitätsverwaltungs-Systeme, der Verzeichnisdienste und des zentralen Identitätsspeichers wird in der IAM-Verordnung (SR 172.010.59) geregelt. In den IAM-Systemen, den Verzeichnisdiensten und dem zentralen Identitätsspeicher dürfen Personendaten bearbeitet werden (Art. 11 Abs. 1 IAMV). Wird ein Informationssystem des Bundes von einem externen Betreiber im Auftrag des Bundes betrieben oder müssen für die Bundesverwaltung tätige Personen auf fremde Informationssysteme zugreifen, so dürfen die dazu notwendigen Personendaten aus Personalinformationssystemen, dem zentralen Identitätsspeicher oder IAM-Systemen automatisiert dem externen Betreiber bekanntgegeben werden (Art. 17 IAMV). Zudem können IAM-Systeme des Bundes als Lieferant von Identitäts- und Authentifizierungsinformationen an ein externes IAM-System oder einen externen Identitätsverbund angeschlossen werden (Art. 24 IAMV).

2.4.7 Abhören und Aufnehmen fremder Gespräche

Artikel 179^{bis}, 179^{ter} und 179^{quater} StGB (SR 311.0) schützen Gesprächsteilnehmende an nichtöffentlichen Gesprächen vor dem unbefugten Abhören und Aufnehmen der Gespräche durch Dritte. Demgemäss regeln die Einsatzrichtlinien UCC (E017) und Microsoft 365 (E031; Verweis auf E017), dass Sprach- und Videoaufzeichnungen zwingend die Zustimmung der Gesprächsteilnehmenden erfordern und unter vollständiger Transparenz des Empfängerkreises der Daten zu erfolgen haben.

Entsprechendes sollte auch für die Funktion des Transkribierens berücksichtigt werden.

2.5 Amtsgeheimnis

Das allgemeine Amtsgeheimnis ist in Artikel 22 Bundespersonalgesetz (BPG; SR 172.220.1) verankert. Für die Angestellten der Bundesverwaltung ergeben sich die Geheimhaltungspflichten darüber hinaus aus zahlreichen allgemeinen und bereichsspezifischen Bestimmungen des Bundesrechts (bspw. Artikel 61 ff. Heilmittelgesetz; SR 812.21). An dieser Stelle wird schwergewichtig die Verletzung des Amtsgeheimnisses gemäss Artikel 320 StGB im Vordergrund stehen, welcher die strafrechtlichen Konsequenzen festlegt.

Microsoft als Cloud-Service Anbieterin hat als Auftragnehmerin zusätzlich eine gesetzliche Treuepflicht. Darüber hinaus können ihr gewisse Geheimhaltungspflichten (insbesondere das

Amtsgeheimnis) explizit überbunden und die Verletzung dieser Pflichten mit hohen Konventionalstrafen belegt werden, so dass das Risiko einer Amtsgeheimnisverletzung auf ein Minimum reduziert werden kann.

3 Schlussfolgerung und Empfehlung

Mit CEBA werden grundsätzlich nicht klassifizierte Daten und Informationen in eine Hybrid-Cloud-Umgebung ausgelagert. Es gibt keine rechtlichen Bestimmungen, die das Verbieten. Um für die Daten und Informationen angemessene Schutzmassnahmen festlegen zu können ist es jedoch wichtig, dass diese vorgängig kategorisiert werden. Diese Massnahmen können je nach Art und Weise der Bearbeitung unterschiedlich ausfallen. Daten können verschlüsselt, anonymisiert oder pseudonymisiert werden. Bei der Bearbeitung der Daten kann der Kreis der Bearbeitenden oder die Art der Bearbeitung eingeschränkt werden oder die Übermittlung der Daten besonders geschützt werden.

Ob Informationen oder Daten ausgelagert werden sollen, ist stets im Einzelfall zu beurteilen. Dazu wurden vorliegend eine Schuban, eine Risikoanalyse und ein ISDS-Konzept erstellt. Die sich aus dieser Prüfung ergebenden Restrisiken wurden ausgewertet und eine Auslagerung der Informationen in M365 mit den oben dargestellten Einschränkungen als vertretbar erachtet.

Daneben können die Risiken auch minimiert werden, indem Microsoft als Cloud-Anbieter folgende vertragliche Pflichten auferlegt werden:

- Das anwendbare Recht ist Schweizer Recht ist und der Gerichtsstand Schweiz (Bern);
- Vertragliche Zusicherung der Wahrung der Geheimhaltungspflichten;
- Zusicherung der Löschung der Daten und Informationen;
- Daten und Informationen jeglicher Art (dazu gehören insbesondere auch Randdaten) dürfen vom Cloud-Anbieter in keiner Weise unbefugt bearbeitet werden.