E031-Einsatzrichtlinie Microsoft 365

Weisung zur Bundesinformatik

Klassifizierung:[1]	Keine
Verbindlichkeit:[2]	Weisung
Vorgabentyp:[3]	(E) Einsatzrichtlinie
Planungsfeld:[4]	Bundesweite IKT-Grundleistungen
Diese Version:	2.2
Ersetzt Version:	2.1
Status (diese Version):	Abgenommen
Beschlussdatum / Datum der Inkraftsetzung (diese Version):	Beschluss zur IKT-Lenkung: 16.06.2025 Inkraftsetzung: 16.06.2025
Erlassen von, Rechtsgrundlage:	Der Delegierte für digitale Transformation und IKT-Lenkung (D-DTI), gestützt auf Artikel 40 der Verordnung vom 1. Mai 2025 über die digitalen Dienste und die digitale Transformation in der Bundesverwaltung (Digitalisierungsverordnung, DigiV), SR 172.019.1
Sprachen:	Deutsch (Original), Französisch (Übersetzung)

[1] Zu den Klassifizierungen INTERN und VERTRAULICH vgl. *Artikel 13 Informationssicherheitsgesetz vom 18. Dezember 2020 (SR 128)*

[2] Zur Erlassform und zur Verbindlichkeit vgl. *Bundesamt für Justiz: Gesetzgebungsleitfaden, 4. Auflage2019 (Stand 2023)*

[3] vgl. Informationsplattform DTI-BK

[4] Planungsfelder gemäss *Strategie Digitale Bundesverwaltung vom 12. Dezember 2023 (SB000)*

Inhaltsverzeichnis

1 Allgemeine Bestimmungen 3

1.1 Gegenstand 3
1.2 Geltungsbereich 3
1.3 Begriffe 3

2 Einsatzrichtlinie Microsoft 365 4

2.1 Verantwortlichkeiten 4
2.2 Datenbearbeitung 5
2.3 Rahmenbedingungen für die Nutzung 6

3 Schlussbestimmungen 7

3.1 Einhaltung 7
3.2 Überprüfung 7
3.3 Inkrafttreten 7

Anhänge 8

A. Nutzung der *M365 Services* 8
B. Übersicht Begrifflichkeiten 10
C. Änderungen gegenüber Vorversion 11
D. Bedeutung der Schlüsselwörter für den Verbindlichkeitsgrad 11
E. Referenzen 11
F. Abkürzungen 12

1 Allgemeine Bestimmungen

1.1 Gegenstand

[1] Diese Weisung regelt die Nutzung der *Microsoft 365-Plattform* als Teil des Standarddienstes Büroautomation.

[2] Die Leistungserbringer LE und die Leistungsbezüger LB (d.h. die Benutzenden) müssen diese Weisung einhalten, damit sie Microsoft 365-Services und die darauf aufbauenden oder erweiternden Dienste nutzen können.[5] Die Einhaltung der Weisung gewährleistet den rechtmässigen Einsatz der M365-Plattform und den Schutz der Daten der Bundesverwaltung.

[3] Sie regelt die Grundsätze zur Bearbeitung der Daten auf der *Microsoft 365-Plattform*. Sie ergänzt bestehende Weisungen des Bundes, der Departemente und weitere Vorgaben der Verwaltungseinheiten zur Nutzung der Informatik. Für die Umsetzung ist sie auf die Mitwirkung und Eigenverantwortung aller Mitarbeitenden der Bundesverwaltung angewiesen.

1.2 Geltungsbereich

[1] **Weisung des Bereichs Digitale Transformation und IKT-Lenkung DTI**

gestützt auf Artikel 40 der Verordnung vom 1. Mai 2025 über die digitalen Dienste und die digitale Transformation in der Bundesverwaltung (Digitalisierungsverordnung, DigiV), SR 172.019.1

[2] Die Weisung ist für die Benutzenden von *M365*-Services des Standarddienst Büroautomation (SD BA) verbindlich.

[3] Der Verbindlichkeitsgrad[6] der einzelnen Bestimmungen in Kapitel 2 dieser Weisung ist gemäss den Schlüsselwörtern in Anhang D festgelegt.

1.3 Begriffe

[1] In dieser Weisung bedeuten:

a. *Microsoft 365-Plattform*: Durch den Standarddienst Büroautomation bereitgestellte Microsoft 365 Public Cloud-Services. Die Plattform ist in die Büroautomationsumgebung der Bundesverwaltung integriert und somit Teil dieser Umgebung.

b. *Microsoft 365 (M365):* Sammlung von Public Cloud basierten Anwendungen und Funktionen für die Büroautomation, wie Teams, SharePoint Online, OneDrive for Business sowie Verwaltungs- und Sicherheitstools, als auch lokal auf dem Arbeitsplatz installierter *Microsoft 365 Apps for Enterprise*.

c. Das *M365 Portfolio Bund* definiert die durch den Standarddienst BA freigegebenen Microsoft 365 Public Cloud-Services.

d. *M365-Services*: Gemäss dem *M365 Portfolio Bund* eingesetzte Services.
Das sind unter anderem folgende:

---

[5] Zum Beispiel Contact Center, Vermittlerarbeitsplatz, Teamschaltungen, Teams Apps, uvm.

[6] Verbindlichkeitsgrade gemäss *Request of Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF).* Die Angabe von Verbindlichkeitsgraden gemäss [RFC 2119] ist eine verbreitete Praxis in der internationalen Standardisierung.

1) *Microsoft 365 Apps for Enterprise (aka M365 Apps)*: Lokal auf dem Arbeitsplatz installierte Büroanwendungen (Teams, Outlook, Word, Excel, PowerPoint, OneNote, Access, usw.).
2) *Microsoft 365*: Cloud-basierte, mit dem Browser nutzbare Büroanwendungen, wie Teams, Outlook Web Access, Word Online, Excel Online, PowerPoint Online.
3) *Exchange Online:* Exchange Online wird für E-Mail-bezogene Dienste genutzt. Der Service ermöglicht den Zugriff auf E-Mails, Kalender, Kontakte und Aufgaben.
4) *Teams:* Cloud-basierte Kollaborations-App. Sie integriert Einzel- und Gruppen-Chat, Video- und Audiokonferenzen, Dokumenten- und Kalenderfreigabe sowie den Erreichbarkeitsstatus der Mitarbeitenden in einem zentralen Arbeitsbereich.
5) *SharePoint Online:* Cloud-basierte Plattform für die Zusammenarbeit. SharePoint Online ermöglicht der Bundesverwaltung die gemeinsame Ablage, Nutzung und Verwaltung von Inhalten und Anwendungen.
6) *OneDrive for Business:* Persönliche cloudbasierte Speicherablage für persönliche und private Daten gemäss Definition [E026]. Geschäftliche Daten sollten, wenn immer möglich, in die gemeinsam genutzten Ablagen bzw. in den hierfür vorgesehenen Systemen gehalten werden.
7) *Viva Engage (früher Yammer):* Soziales Netzwerk, welches im Unternehmenskontext eingesetzt wird. Durch den beruflichen Fokus stehen das Teilen und die Bearbeitung von Dokumenten, der Austausch von Wissen sowie die unternehmensinterne und unternehmensübergreifende Zusammenarbeit und Kommunikation im Vordergrund. Bundesintern wird es vor allem für sogenannte «Communities of Practice» eingesetzt.

e. *Account Modern:* Ein Benutzeraccount gemäss dem Servicekatalog SD, welcher im On-Premises Active Directory geführt und in das Azure Active Directory repliziert wird. Erst mit dem *Account Modern* stehen die M365-Services zur Verfügung.
f. *Arbeitsplatzsystem bzw. Arbeitsplatz:* Das Arbeitsplatzsystem besteht aus dem Service "Arbeitsplatz" [SD105] und dem Service «Virtueller Desktop» [SD119], welcher im SD BA gemäss dem Servicekatalog der Standarddienste [SD100] angeboten wird. Das Arbeitsplatzsystem ist in die Büroautomationsumgebungen des Bundes eingebunden und ermöglicht den Zugriff auf die Fachanwendungen des Bundes.

[2] Eine Übersicht der Begrifflichkeiten und der Geltungsbereich sind im Anhang B grafisch dargestellt.

2 Einsatzrichtlinie Microsoft 365

2.1 Verantwortlichkeiten

[1] Der Standarddienst Büroautomation stellt zusammen mit den definierten LE die standardisierten und zentralisierten IKT-Grundleistungen des Arbeitsplatzes gemäss Servicekatalog der Standarddienste [SD100] sicher.

[2] Der Standarddienst Büroautomation sorgt für die Bereitstellung der *M365-Services* und stellt den IT-Grundschutz [Si001] sicher.

[3] Die Departemente und Verwaltungseinheiten (Leistungsbezüger) kennen die Daten und die Geschäftsprozesse, welche sie mit M365 bearbeiten wollen. Sie sind mit den geltenden Vorgaben für ihre Bereiche vertraut. Sie MÜSSEN daher den Schutzbedarf der Daten in eigener Verantwortung bestimmen. Sie prüfen, ob die IT-Grundschutzmassnahmen, für die von ihnen zu verantwortenden Daten ausreichen. Sie müssen insbesondere sicherstellen, dass keine unerlaubten Daten gemäss Kapitel 2.2 Abs. 1 auf M365 bearbeitet werden.

[4] Die bearbeiteten Dokumente MÜSSEN durch die Benutzenden oder durch automatisierte Prozesse entsprechend ihrer Klassifizierung nach Informationssicherheitsgesetz [ISG] und Datenschutzgesetz {DSG] eingestuft bzw. mit einem entsprechenden Label versehen werden.

[5] Die Departemente und Verwaltungseinheiten (Leistungsbezüger) legen bei Bedarf für ihren Verantwortungsbereich weitergehende Vorgaben und Massnahmen fest.

[6] Der Standarddienst Büroautomation unterstützt die Departemente und Verwaltungseinheiten dabei (namentlich mit IKT-Werkzeugen, Hilfsmitteln, Schulungsangeboten, etc.), die Verantwortung gemäss Abs. 3 übernehmen zu können.

[7] Externe Benutzer (Gäste) DÜRFEN zur Zusammenarbeit eingeladen werden. Hierbei MUSS es sich um einen geschäftlichen Kontext handeln und die einladende Person (Bundesmitarbeiter/in) MUSS die Identität der Person sicherstellen. Die mit der Einladung vergebenen Zugriffsberechtigungen MÜSSEN von der einladenden Person vierteljährlich überprüft und dem externen Benutzenden gegebenenfalls entzogen werden, wenn sie nicht mehr benötigt werden.

2.2 Datenbearbeitung

[1] Mit M365 DÜRFEN «nicht klassifizierte Informationen» nach Informationssicherheitsverordnung [ISV] sowie «Personendaten» nach Datenschutzgesetz [DSG] bearbeitet werden.

Für höher klassifizierte Informationen nach ISV bzw. «besonders schützenswerte Personendaten» sowie «Profiling» nach DSG sind die M365-Services, mit Ausnahmen[7], nicht zugelassen. Diese Daten müssen mit der lokal installierten Office-Version und den dafür freigegebenen Werkzeugen[8] geöffnet und bearbeitet werden. Sie sind auf den für die Verwaltungseinheit freigegebenen Diensten wie z.B. GEVER oder Fachanwendungen zu speichern.

Die aktuell zugelassene Nutzung der einzelnen M365-Services ist im Anhang A aufgeführt.

[2] Sofern kein Datenbearbeitungsreglement oder eine Vorgabe der Verwaltungseinheit es verbietet, DÜRFEN unter das Amtsgeheimnis fallende Informationen mit M365-Services bearbeitet werden.[9]

---

[7] Als Ausnahme darf MS-Teams mit Anwendung der Ende-zu-Ende-Verschlüsselung für besonders schützenswerte Personendaten nach DSG und INTERN klassifizierte Informationen nach ISV eingesetzt werden.

[8] Zurzeit sind das u.a. die Verschlüsselungswerkzeuge SecureCenter und das Nachfolgeprodukt CHCrypt

[9] Entsprechend den Ausführungen in der Rechtsgrundlagenanalyse zu Microsoft 365 ist die Bearbeitung von unter das Amtsgeheimnis fallenden Daten, basierend auf den abgeschlossenen Verträgen mit Microsoft und der vorgenommenen Gesetzesänderung im Art. 320 StGB, erlaubt (Verweis: Projekt CEBA → Weiterführende Unterlagen (Bereich Dokumente)).

Im Dokument «Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung» [Si001-Hi03] sind die Handlungsempfehlungen zur Verhinderung von Amtsgeheimnisverletzungen beschrieben, die allenfalls im Zusammenhang mit der Weitergabe von Daten an Dritte bei Supportfällen relevant werden. Im Zweifelsfall ist es sinnvoll zur Beurteilung den Rechtsdienst der Verwaltungseinheit beizuziehen.

[3] Die Departemente und/oder Verwaltungseinheiten SOLLEN ihren Mitarbeitenden Hilfestellungen zur Klassifizierung von Informationen sowie Einstufung nach DSG geben. Da nur die Verwaltungseinheiten ihre Geschäfte und Inhalte kennen, DÜRFEN sie organisationsspezifische Regelungen für die Nutzung von M365 festlegen.

[4] Die *M365-Services* SOLLEN gemäss der Einsatzrichtlinie Arbeitsplatzsystem [E026] für geschäftliche Zwecke eingesetzt werden.

[5] Die Benutzenden DÜRFEN geschäftsrelevante Informationen mit M365-Services temporär bearbeiten. Nach Abschluss der Arbeiten MÜSSEN diese in das jeweilige Geschäftsverwaltungssystem GEVER oder Fachanwendung der Verwaltungseinheit zurückgeführt werden.[10]

[6] Für die Besprechung von «besonders schützenswerten Personendaten» oder INTERN klassifizierte Informationen mit Microsoft Teams sowie Aufzeichnung der Sprach- und/oder Videokommunikation MUSS die Einsatzrichtlinie [E017] berücksichtigt werden.

[7] Zu jeder *Viva Engage* Unterhaltung MUSS mindestens ein Moderator definiert werden, welcher bei Bedarf in die Diskussionen eingreift (z.B. Beschimpfungen, Rassismus, Diskriminierung).

[8] In Teams Besprechungen DÜRFEN Transkriptionen vorgenommen werden. Die Teilnehmenden der Besprechung MÜSSEN darüber und über die weitere Bearbeitung der Transkription informiert sein. Bei einer verschlüsselten Kommunikation mit Teams ist die Transkription technisch nicht möglich.

2.3 Rahmenbedingungen für die Nutzung

[1] Die M365-Services werden, wenn immer dies von Microsoft angeboten wird, innerhalb der Schweiz betrieben und die Daten auf Schweizer Territorium gehalten. Wo dies nicht möglich ist, werden die Dienste im Raum der Europäischen Union (EU Data Boundary) betrieben.[11]

[2] Aus beschaffungsrechtlicher Sicht oder aufgrund sicherheitsrelevanter Bedenken stehen gewisse M365-Services nicht zur Verfügung. Der zur Verfügung stehende Funktionsumfang ist im *M365 Portfolio Bund* definiert.

[3] Für die Nutzung der *M365*-Services bestellt die VE gemäss Servicekatalog SD die Marktleistung «*Account Modern»*.

[4] Smartdevices, welche über das Mobile Devices Management der LE verwaltet werden, DÜRFEN M365-Services ohne Einschränkung nutzen.
Alle anderen Privat- oder Fremdgeräte DÜRFEN die M365-Services nur über die Online-Bearbeitung (Office Online) via Browser nutzen.[12]

[5] Der vollwertige Zugang zu M365-Services (Login) MUSS durch die freigegebenen Authentifikationsmittel (z.B. Smartcard oder andere Multifaktor-Authentifizierungen) erfolgen.[13]

[6] Bei der ersten Anmeldung auf der *M365-Plattform* MÜSSEN die Benutzenden bestätigen, dass Sie diese Einsatzrichtlinie zur Kenntnis genommen haben und einhalten.

---

[10] Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung, SR 172.010.441) Artikel 4

[11] Informationen, wo Microsoft 365 die Kundendaten speichert: https://learn.microsoft.com/de-de/microsoft-365/enterprise/o365-data-locations?view=o365-worldwide

[12] Siehe auch Anhang A Tabelle 2. Dies wird vom Leistungserbringer auch technisch umgesetzt

[13] Dies wird vom Leistungserbringer auch technisch umgesetzt

3 Schlussbestimmungen

3.1 Einhaltung

[1] Die Departemente und die Bundeskanzlei sorgen gemäss DigiV für die Umsetzung dieser Weisungen in ihrem Zuständigkeitsbereich.

3.2 Überprüfung

[1] Der Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei (Bereich DTI) überprüft die Aktualität und Zweckmässigkeit dieser Weisung spätestens vier Jahre nach deren Inkraftsetzung.

3.3 Inkrafttreten

[1] Diese Weisung tritt in der hier vorliegenden Version am 16.06.2025 in Kraft.

[2] Für die CEBA Agil Plattform bleibt die Version 1.1 bis zur Ausserbetriebnahme von CEBA Agil gültig.

Anhänge

A. Nutzung der *M365 Services*

Die folgenden Tabellen zeigen die Nutzungsmöglichkeiten der wichtigsten ***M365 Services*** bezüglich der Informations- und Datenschutzaspekte auf.
Die Vorgaben und Einschränkung für die Klassifikation INTERN nach ISV, werden nach Vorliegen der Bearbeitungsvorschriften vom SEPOS neu geprüft.

Grün: ohne Einschränkung erlaubt gelb: mit Einschränkungen erlaubt rot: nicht erlaubt

Einstufung DSG	**Einstufung ISV**	**Lokale Office Anwendungen (auf APS installiert)**	**M365 Online (Office Web-Version)**	**Teams**	**SharePoint Online**	**OneDrive for Business**	**Viva Engage**	**Alle andern** (wie z.B. Planner, To Do List, …)
Personen-daten	**Nicht klassi-fiziert**	Ohne Einschränkung	Ohne Einschränkung auf ver-walteten Endgeräten (APS) Nur Online-Bearbeitung auf nicht verwalteten Endgeräten (z.B. Privat-PC)	Ohne Einschränkung	Ohne Einschränkung	Ohne Einschränkung	Ohne Einschränkung	Ohne Einschränkung
Besonders schützens-werte Personenda-ten				Unter Anwendung der Ende-zu-Ende Ver-schlüsselung (weiterer führende Informatio-nen in der **E017**) dürfen während der Sprach- und/oder Videokommunikation «besonders schützenswerte Personenda-ten» ausgetauscht werden. Eine Transkription ist nicht möglich. Der Austausch per **Chat** ist nicht zugelassen.				
	INTERN	Eine Bearbeitung ist auf dem APS uneinge-schränkt möglich. Die Informationen müssen jedoch auf On-Premises-Systemen wie GEVER oder von der VE freigegebene Ablage bzw. Anwen-dung gespeichert werden. Eine Speicherung in M365 ist nicht zulässig.	Keine Bearbeitung zugelas-sen	Unter Anwendung der Ende-zu-Ende Ver-schlüsselung (weiterer führende Informatio-nen in der **E017**) dürfen während der Sprach- und/oder Videokommunikation IN-TERN klassifizierte Informationen ausge-tauscht werden. Eine Transkription ist nicht möglich. Der Austausch per **Chat** ist nicht zugelassen.	Keine Bearbei-tung und Spei-cherung zuge-lassen	Keine Speicherung zugelassen	Keine Bearbeitung und Speicherung zu-gelassen	Keine Bearbeitung und Speicherung zu-gelassen
Besonders schützens-werte Personenda-ten und Profiling	**VERTRAU-LICH**	Dokumente müssen mit freigegebener Ver-schlüsselung[14] geschützt sein. Bearbeitung nur in der lokalen SAFE-Area der Verschlüsselungsumgebung. Ablage in GEVER oder in von der VE freige-gebenen Ablage oder Anwendung.	Keine Bearbeitung zugelas-sen	Keine Bearbeitung, Speicherung und Chat-/Audio-/Video-Kommunikation zugelassen	Keine Bearbei-tung und Spei-cherung zuge-lassen	Keine Speicherung zugelassen	Keine Bearbeitung und Speicherung zu-gelassen	Keine Bearbeitung und Speicherung zu-gelassen
	GEHEIM	Nicht erlaubt	Nicht erlaubt	Nicht erlaubt	Nicht erlaubt	Nicht erlaubt	Nicht erlaubt	Nicht erlaubt

Tabelle 1: Nutzungsmöglichkeiten der M365 Services

[14] Eine freigegebene Verschlüsselung ist z.B. Secure Center bzw. CHCrypt

Nutzungsmöglichkeiten von M365 Services auf den Endgerätekategorien

Die folgende Tabelle zeigt die Nutzungsmöglichkeiten aus der Sicht der unterschiedlichen Endgerätekategorien auf. M365 Services dürfen auf vom Bund verwalteten Endgeräten für Personendaten und nicht klassifizierte Informationen ohne Einschränkung genutzt werden. Von Fremdgeräten aus ist der Zugang auf M365 entweder über den mobile VDI-Service oder via Browser (nur Online Tools nutzbar) möglich. Der Zugang wird mit dem Bundesaccount und einer freigegebenen Multi Faktor Authentifizierung erlangt. Für höher eingestufte Daten gelten generell Einschränkungen oder sind nicht erlaubt.

		Endgerät		
Einstufung gemäss DSG	**Einstufung gemäss ISV**	**Vollständig verwalteter APS** (BA-Client) mit lokal installierten Office Anwendung und OneDrive for Business (inkl. mobile VDI)	**Teilweise verwaltetes** Endgerät mit MDM des Bundes, wie Smartdevice mit lokal installierten Office Mobile Anwendungen und OneDrive for Business	**Nicht verwaltetes Fremdgerät** (z.B. Privat-PC, BYOD, privates Smartphone ohne MDM)
Personendaten	**Nicht klassifiziert**	**Ohne Einschränkung nutzbar**	**Ohne Einschränkung nutzbar**	Nur Online-Bearbeitung auf M365 via Browser möglich (M365 Office Online; mit Bundesaccount und MFA) Ausnahme: mobile VDI: ohne Einschränkung nutzbar
Besonders schützenswerte Personendaten	**Nicht klassifiziert**	Führen von Sprach- und/oder Videokommunikation unter Anwendung der Ende-zu-Ende Verschlüsselung (Verweis E017). Für «besonders schützenswerte Personendaten» ist aber der Austausch per Chat nicht zugelassen	Führen von Sprach- und/oder Videokommunikation unter Anwendung der Ende-zu-Ende Verschlüsselung (Verweis E017). Eine Transkription ist nicht möglich Für «besonders schützenswerte Personendaten» ist aber der Austausch per Chat nicht zugelassen.	Führen von Sprach- und/oder Videokommunikation unter Anwendung der Ende-zu-Ende Verschlüsselung (Verweis E017). Für «besonders schützenswerte Personendaten» ist aber der Austausch per Chat nicht zugelassen
	INTERN	Eine Bearbeitung ist auf dem APS uneingeschränkt möglich. Die Informationen müssen jedoch auf On-Premises-Systemen wie GEVER oder von der VE freigegebene Ablage bzw. Anwendung gespeichert werden. Eine Speicherung in M365 oder OneDrive for Business ist nicht zulässig.	Führen von Sprach- und/oder Videokommunikation unter Anwendung der Ende-zu-Ende Verschlüsselung (Verweis E017). Eine Transkription ist nicht möglich und der Austausch per Chat ist nicht zugelassen. Eine Bearbeitung ist auf dem MDM integrierten Smartphone uneingeschränkt möglich. Die Informationen müssen jedoch auf On-Premises-Systemen wie GEVER oder von der VE freigegebene Ablage bzw. Anwendung gespeichert werden. Eine Speicherung in M365 oder OneDrive for Business ist nicht zulässig.	Keine Bearbeitung, Speicherung und Chat-/Audio-/Video-Kommunikation mit Teams zugelassen Ausnahme: Eine Bearbeitung ist auf mobile VDI uneingeschränkt möglich. Die Informationen müssen jedoch auf On-Premises-Systemen wie GEVER oder von der VE freigegebene Ablage bzw. Anwendung gespeichert werden. Eine Speicherung in M365 oder OneDrive for Business ist nicht zulässig.
Besonders schützenswerte Personendaten und Profiling	**VERTRAULICH**	Dokumente müssen mit freigegebener Verschlüsselung geschützt sein. Bearbeitung nur in der lokalen «SAFE-Area» der Verschlüsselungsumgebung. Ablage in GEVER oder in von der VE freigegebenen Ablage oder Anwendung. Audio-/Video- und Chat-Kommunikation sind mit Teams nicht erlaubt.	Keine Bearbeitung, Speicherung und Chat-/Audio-/Video-Kommunikation mit Teams zugelassen (es besteht keine Integration mit dem Verschlüsslungstool)	Keine Bearbeitung, Speicherung und Chat-/Audio-/Video-Kommunikation mit Teams zugelassen (es besteht keine Integration mit dem Verschlüsslungstool)

Tabelle 2: Darstellung der Nutzung der M365 Services aus Sicht Endgeräte

B. Übersicht Begrifflichkeiten

Die Einsatzrichtlinie E031 bezieht sich auf die Nutzung der Microsoft 365 Plattform, die in der Abbildung ausgefüllt gekennzeichnet ist. Hierbei handelt es sich um eine schematische Abgrenzung zwischen der Microsoft 365 Plattform und den bestehenden Büroautomationsdiensten der Bundesverwaltung. Die Grafik zeigt die Zusammenhänge der verwendeten Begrifflichkeiten auf.

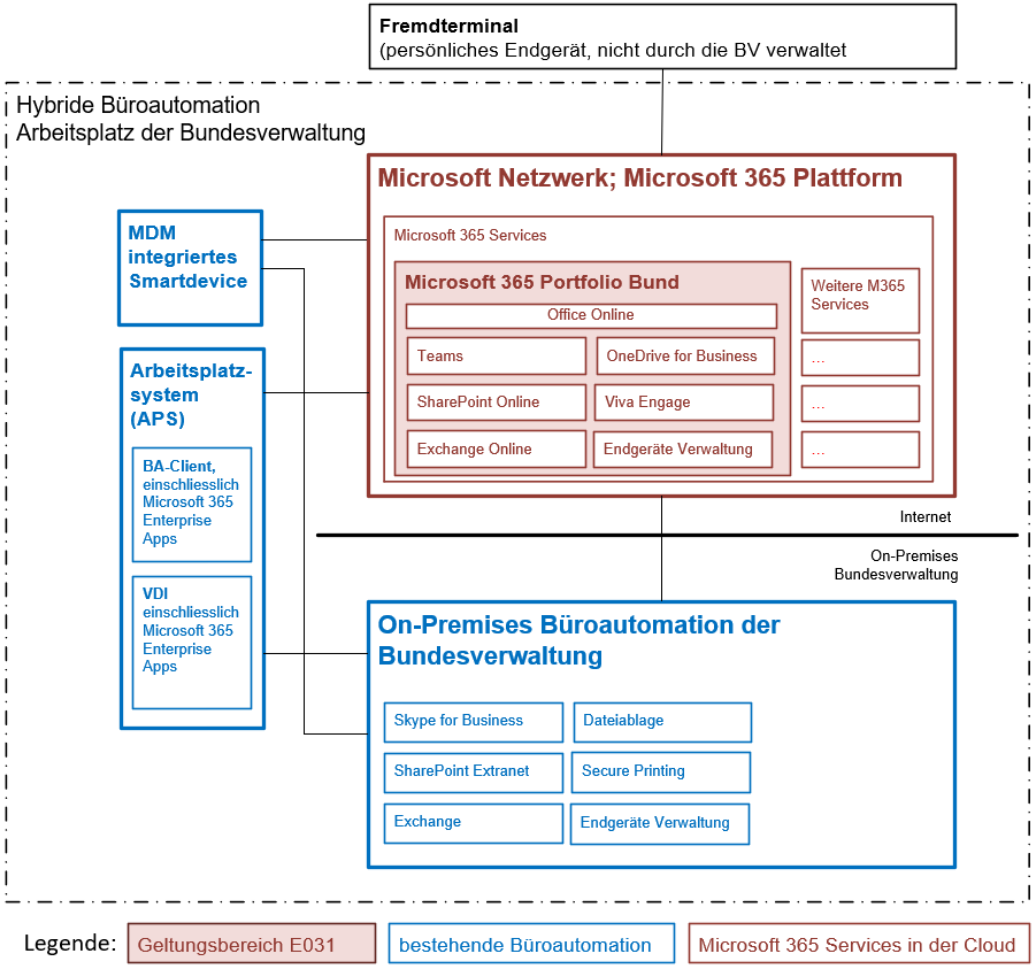

Abbildung 1: Übersicht Begrifflichkeiten

C. Änderungen gegenüber Vorversion

- Verweis auf die Einsatzrichtlinie [E017] zur Besprechung von «besonders schützenswerten Personendaten» gemäss DSG und INTERN klassifizierten Informationen nach ISV mit Microsoft Teams sowie zur Aufzeichnung von Sprach- und/oder Videokommunikation.
- Anpassung der Tabelle in Anhang A (Ergänzung zur Führung von Gesprächen mit «besonders schützenswerten Personendaten» gemäss DSG unter Anwendung von Ende-zu-Ende Verschlüsselung).
- Aufführung der Verantwortlichkeiten der Einladenden gegenüber dem Gast.
- VDTI durch DigiV ersetzt

D. Bedeutung der Schlüsselwörter für den Verbindlichkeitsgrad

Der Verbindlichkeitsgrad[15] der einzelnen Bestimmungen in Kapitel 2 dieser Weisung wird mittels folgender Schlüsselwörter in Grossbuchstaben gekennzeichnet:

Schlüsselwort	**Verbindlichkeitsgrad**
MUSS	Bestimmung, die zwingend einzuhalten ist (gewährte Ausnahmen ausgenommen)
DARF NICHT	Option, die nicht gewählt werden darf
DARF	Option ist ausdrücklich erlaubt. Die VE kann entscheiden, ob sie die Option nutzen möchte oder nicht. Betrifft die Bestimmung eine IKT-Lösung, muss der Anbieter dieser Lösung die Wahlmöglichkeit anbieten.
SOLL	Option, die im Normalfall zu wählen ist. Eine VE kann jedoch ohne Ausnahmegewährung des Bereich DTI-BK bzw. des NCSC davon abweichen, wenn dadurch Wirtschaftlichkeit und/oder Sicherheit nicht beeinträchtigt werden. Die Abweichung von der Bestimmung ist gegenüber dem Bereich DTI-BK bzw. dem NCSC schriftlich zu begründen.
KANN	Akzeptierte Option. Betrifft die Vorgabe eine IKT-Lösung, entscheidet der Anbieter der IKT-Lösung darüber, ob er die Option unterstützen will.

E. Referenzen

ID	**Referenz[16]**
DSG	Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992 (Stand am 1. September 2023); SR 235.1
E026	E026 – Einsatzrichtlinie Arbeitsplatzsystem

[15] Verbindlichkeitsgrade gemäss *Request for Comments: RFC 2119 (PCB 14), The Internet Engineering Task Force (IETF).* Die Angabe von Verbindlichkeitsgraden gemäss [RFC 2119] ist eine verbreitete Praxis in der internationalen Standardisierung.

[16] Erlasse auf Bundesstufe werden gemäss der «Systematischen Rechtssammlung» referenziert. Bei einer referenzierten Bundesvorgabe wird die zum Beschlussdatum dieser Weisung gültige Version angegeben.

ID	Referenz[16]
GEVER-Verordnung	Verordnung über die elektronische Geschäftsverwaltung in der Bundesverwaltung (GEVER-Verordnung); SR 172.010.441
ISG	Bundesgesetz über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG); AS 2022 232
ISV	Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung) AS 2023 735
RFC 2119	Request for Comments: 2119 (PCB14), The Internet Engineering Task Force (IETF)
SB000	SB000 – IKT-Strategie des Bundes 2020–2023
SD100 - Servicekatalog SD	Der Servicekatalog der IKT-Standarddienste (SD) führt die innerhalb der Standarddienste erbrachten Service, Service-Varianten und -Optionen auf. Er richtet sich in erster Linie an die Integrationsmanager der Departemente (IMD) sowie an die Leistungserbringer der Standarddienste (LE-SD). SD100 - Servicekatalog SD
Si001	Si001 - IT-Grundschutz in der Bundesverwaltung
Si001-Hi3	Si001 - Hi03: Anforderungen angesichts des Risikos von Amtsgeheimnisverletzungen in der Bundesverwaltung – Version 1.4
StGB Art 320 (Amtsgeheimnis	Ein Amtsgeheimnis liegt dann vor, wenn eine gesetzliche Geheimhaltungspflicht besteht und es sich um Tatsachen handelt, die weder öffentlich bekannt noch allgemein zugänglich sind und welche weder im öffentlichen noch im privaten Interesse mitgeteilt werden dürfen (Verweis StGB 320 Abs. 1).
DigiV	Digitalisierungsverordnung, SR 172.019.1

F. Abkürzungen

Kürzel	Bedeutung
BA	Büroautomation
BK	Bundekanzlei der Schweizerischen Eidgenossenschaft
CEBA	Programm Cloud Enabling Büroautomation
DSG	Datenschutzgesetz
DTI	Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei
GEVER	Geschäftsverwaltung
ISG	Informationssicherheitsgesetz
ISV	Informationssicherheitsverordnung
IKT	Informations- und Kommunikationstechnologie
MDM	Mobile Device Management
NCSC	Nationales Zentrum für Cybersicherheit
SD BA	Standarddienst Büroautomation
RFC	Request for Comments
VE	Verwaltungseinheit