

Betriebsvereinbarung

über die Einführung und Anwendung von Microsoft 365 gemäß §§ 96, 96a und 97 ArbVG

Präambel

Microsoft 365 ist die Produktfamilie für Cloud- und on-premises Anwendungen von Microsoft und beinhaltet folgenden Anwendungsbereiche:

- Office 365
- Enterprise Mobility + Security (EMS)
- Windows Enterprise
- (Dynamics 365)

[Die Produktlinie Dynamics 365 ist zwar kein unmittelbarer Teil von Microsoft 365, werden jedoch einzelne Komponenten daraus eingesetzt, können diese ebenfalls im Rahmen dieser Vereinbarung (oder aber gesondert) geregelt werden.]

Diese Plattform Produkt wird laufend erweitert¹, daher kann nur der betrieblich anhand der Checkliste (siehe **Beilage**) dokumentierte Ist-Stand die Grundlage für diese Betriebsvereinbarung sein, wobei parallel die Einbeziehung des Betriebsrates bei der betrieblichen Erweiterung festzuschreiben ist. Aus diesem Grund wird diese Betriebsvereinbarung befristet abgeschlossen, wobei die Möglichkeit besteht, diese jeweils an aktuelle Veränderungen anzupassen bzw. sofern keine Veränderungen im Beobachtungszeitraum stattfinden, eine auslaufende Befristung zu verlängern.

Bezüglich des datenschutzrechtlichen Einsatzes von Microsoft 365 verpflichtet sich das Unternehmen (Arbeitgeber) als datenschutzrechtlicher Verantwortlicher, die Aktivitäten des Europäischen Datenschutzbeauftragten bzw. der nationalen Datenschutzbehörde(n) - im Hinblick auf Prüfungen der bezugnehmenden Microsoft Services und Produkte - zu verfolgen und auf Grundlage deren Empfehlung bzw. Entscheidungen daraus resultierende notwendige vertragliche oder datenschutzrechtliche Schritte mit dem Betriebsrates zu vereinbaren.

Darüber hinaus ist seitens des Unternehmens (Arbeitgeber) als datenschutzrechtlicher Verantwortlicher folgende Dokumentation aktuell zu halten:

- a) Einhaltung der Grundsätze zur Datenverarbeitung nach Art 5 DSGVO bei Start und Veränderung von Microsoft 365
- b) Abschätzung des Risikos bei Einsatz und Erweiterungen von Microsoft 365
- c) Verzeichnis der Verarbeitungstätigkeit nach Art 30 DSGVO
- d) Information an MitarbeiterInnen (Transparenzgebot)

¹ Siehe z.B. <https://m365maps.com/>

1. GELTUNGSBEREICH

Die Betriebsvereinbarung gilt für alle Beschäftigte der [Unternehmen einfügen].

Alle in dieser Betriebsvereinbarung beigefügten Anlagen bilden, sofern sie nicht ausschließlich informativen Charakter besitzen [dies wäre gesondert zu kennzeichnen], einen integrierenden Bestandteil dieser Vereinbarung und können nur im beiderseitigen Einverständnis geändert werden.

[sofern zutreffend: Bestehende Betriebsvereinbarungen zu verschiedenen bereits im Einsatz befindlichen Microsoft 365 Modulen bzw. Services, werden nach beiderseitiger Prüfung der Aktualität durch die Vertragsparteien in die Anlage aufgenommen bzw. überarbeitet.

[sofern zutreffend: Die Regelungen der Rahmen-Betriebsvereinbarung zur personenbezogenen Datenverarbeitung gelten sinngemäß, sofern in dieser Vereinbarung nicht Abweichendes vereinbart wurde]

2. ZIEL

Ziele dieser Betriebsvereinbarung sind

- einen Überblick der eingesetzten betriebsvereinbarungsrelevanten Komponenten von Microsoft 365 (Office 365, EMS, Windows Enterprise) zu erhalten
- über Anhänge die zweckgebundene Verarbeitung personenbezogener Daten der MitarbeiterInnen in den zum Einsatz gelangenden Komponenten festzuhalten
- die Erfüllung der datenschutzrechtlichen (DSGVO/GDPR, DSG) und arbeitsrechtlichen (ArbVG) Anforderungen zu beschreiben
- der Schutz der Persönlichkeitsrechte der Beschäftigten (Betroffene nach DSGVO/GDPR) im Zusammenhang mit der elektronischen Personaldatenverarbeitung sowie die Erfüllung des Transparenzgebotes über die Ermittlung, Verarbeitung und Übermittlung personenbezogener Daten (nach Art 4 Z 1 DSGVO/GDPR),
- der Schutz der Beschäftigten vor den Gefahren einer technischen Überwachung ihrer Leistung oder ihres Verhaltens sowie
- Regeln für die Weitergabe von personenbezogenen Daten.

3. KURZBESCHREIBUNG DES SYSTEMS

Von Microsoft 365 werden die in **Beilage** angeführten Komponenten genutzt, somit bildet diese Beilage einen informativen Überblick zum technischen, datenschutzrechtlichen und organisatorischen Ist-Stand [-> siehe Beilage Checkliste!] und ist bei Veränderungen dem Betriebsrat in aktualisierter Form zu übermitteln.

Das Unternehmen sichert als datenschutzrechtlicher Verantwortlicher zu, die Anforderungen der DSGVO/GDPR im Hinblick auf die Grundsätze für die Verarbeitung von personenbezogenen Daten der Beschäftigten (insb. Rechenschaftspflicht) nach Art 5 DSGVO/GDPR geprüft und die daraus resultierenden Dokumentationspflichten umgesetzt zu haben. Diese Informationen sind dem Betriebsrat aufgrund und unter Einhaltung der Bestimmungen der §§ 89, 91, 96, 96a und 97 ArbVG zur Verfügung gestellt worden.

Diese Informationspflicht umfasst auch eine aktuelle Darstellung über die zum Einsatz gelangende Infrastruktur (Verarbeitung in der cloud, hybride Umsetzung) und die daraus resultierenden Auftragsverarbeiterverträge (zumindest die datenschutzrechtlich relevanten Abschnitte).

Ein Zugriff auf die Microsoft 365 Umgebung ist sowohl mit dienstlichen als auch privaten [zu prüfen] Geräten (PC, Laptop, Tablet Smartphone) möglich, wobei die im Unternehmen dazu vereinbarten, geschulten und in der Anlage angeführten Sicherheitsmaßnahmen [Verweis auf betriebsinternes Dokument, z.B. IT-Policy, ...] einzuhalten sind.

Eine betriebliche Erweiterung der Microsoft 365 Komponenten (Apps, Services), wie in der Beilage Checkliste dargestellt, bedarf jedenfalls der vorherigen Information des Betriebsrates und nach Prüfung der datenschutz- und arbeitsrechtlichen Anforderungen gegebenenfalls der Erweiterung dieser Betriebsvereinbarung bzw. deren Anlagen.

4. DATENVERARBEITUNG

In **Anlage 1** sind die personenbezogenen Daten angeführt, die von Beschäftigten grundsätzlich bei der Nutzung von Microsoft 365 verarbeitet werden.

Dabei wird unterschieden in

- **Stammdaten** zu den Beschäftigten
- **Funktionsdaten**, die zur Einrichtung der Services/Komponenten notwendig sind
- **(Inhalts)Daten**, die durch das individuelle Arbeiten der Beschäftigten in den unterschiedlichen Services/Komponenten entstehen
- **Verhaltensdaten**, diagnostische Daten, Protokoll-, Verkehrs- und Telemetriedaten, die im Hintergrund der Services/Komponenten anfallen

Eine personenbezogene Datenverarbeitung ist zur Nutzung der Komponenten von Microsoft 365 notwendig.

Personenbezogene Auswertungen und Analysen finden jedoch ausschließlich in folgenden Fällen statt:

- Die personenbezogenen Einzeldaten werden in aggregierter Form dargestellt,
- der Betriebsrat hat für einen konkreten Einzelfall seine Zustimmung gegeben,
- die personenbezogene Auswertung ist in dieser Vereinbarung oder einer Anlage zu dieser Vereinbarung angeführt.

Sofern nicht ausdrücklich vereinbart, ist jedenfalls jegliche Art der automatisierten Verarbeitung personenbezogener Daten, unter Bewertung der persönlichen Aspekte eines/r ArbeitnehmerIn, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel ausgeschlossen (Profilingverbot).

Unternehmen und Betriebsrat definieren unter Beachtung der Bestimmungen der Arbeitsverfassung diejenigen Services/Komponenten (siehe dazu Überblick in der Beilage Checkliste), deren Einsatz in einer gesonderten Anlage zu dieser Betriebsvereinbarung zu dokumentieren ist, wobei zumindest folgende Inhalte zu vereinbaren sind:

- Zweck der Datenverarbeitung
- Auflistung der dabei verarbeiteten personenbezogenen Daten, sofern diese nicht bereits Teil von Anlage 1 sind (zB da diese ausschließlich für den dokumentierten Service von Bedeutung sind)
- vereinbarte personenbezogene Auswertungen und Analysen
- Schnittstellen zu anderen (Nicht-Microsoft-) Systemen
- Übermittlung von Daten an betriebsexterne Empfänger
- Rollen- und Berechtigungskonzept

5. SYSTEMADMINISTRATION

Die Nutzung der Microsoft 365 Applikationen wird ausschließlich in aggregierter Form aufbereitet, d.h. es dürfen keine Daten von Personengruppen mit weniger als 6² [bzw. betrieblich vereinbarte Mindestgröße einfügen] Personen dargestellt werden. Der Rückschluss auf das Nutzungsverhalten einzelner Beschäftigte sowie deren Identität ist somit anhand dieser Daten nicht gestattet, außer es wird in dieser Vereinbarung bzw. einer Anlage zu dieser Vereinbarung Abweichendes vereinbart.

Ausgenommen davon ist einzig die Prüfung der Berechtigung zur Nutzung der einzelnen Applikationen (z.B. Lizenz).

Der Umgang mit Telemetrie-Daten in Office 365 oder Windows Enterprise ist betrieblich festzuschreiben.

Eine Auswertung von personenbezogenen Aktivitäten (Logs, Verhaltensdaten oder dgl.) der Benutzer in den anderen Microsoft 365 Komponenten ist somit nur in der in der Anlage definierten Form gestattet.

Alle genutzten Analysen des Verhaltens sind gegenüber den betroffenen Beschäftigten in transparenter Form darzustellen.

Mit allen zugriffsberechtigten Administratoren wurden Vereinbarungen zur Wahrung des Datengeheimnisses gemäß DSGVO/GDPR bzw. § 6 DSG abgeschlossen und diese Personen werden nachweislich von den Regelungen dieser Vereinbarung informiert.

6. AUFTRAGSVERARBEITER (DIENSTLEITER)

Alle Auftragsverarbeiter sind zur Einhaltung der datenschutzrechtlichen Bestimmungen zu verpflichten.

Dies betrifft auch die Vereinbarung mit Microsoft bzw. deren autorisierten Partnern (insbesondere die Online Service Terms OST).

Verarbeiten Auftragsverarbeiter personenbezogene Daten sind sie darüber in Kenntnis zu setzen, keine dieser Betriebsvereinbarung widersprechende Daten zu übermitteln oder zur Verfügung zu stellen. In diesen Fällen sind auch die Zugriffsrollen zu beschreiben.

2 Diese Gruppengröße wird von der österreichischen Datenschutzbehörde (damals Datenschutzkommission) empfohlen, siehe: <http://tinyurl.com/K213-180> und <http://tinyurl.com/DSB-D215-611>

Der Betriebsrat erhält auf Anforderung Einsicht in die dazu relevanten Passagen der Verträge.

Darüber hinaus erhält der Betriebsrat eine Übersicht der an Auftragsverarbeiter oder sonstige betriebsfremde Dritte (dazu können auch andere Konzerntöchter bzw. die Konzernmutter fallen) vergebenen Berechtigungsrollen und die damit verbundenen Möglichkeiten personenbezogene Beschäftigtendaten zu verarbeiten.

7. VERSTÖßE GEGEN DIESE BETRIEBSVEREINBARUNG

Werden Verstöße gegen diese Betriebsvereinbarung bekannt (z.B. nicht vereinbarte Auswertungen, unberechtigte Weitergabe von Informationen), kann dies (dienst)rechtliche Maßnahmen nach sich ziehen.

Daten, die die Leistung und/oder das Verhalten von Beschäftigten beschreiben und unter Umgehung der in dieser Vereinbarung bzw. Anlagen beschriebenen Abläufe erhoben oder verarbeitet werden, dürfen – sofern sie nicht strafrechtliche Bedeutung besitzen - nicht als Beweismittel für personeller Maßnahmen verwendet werden, es gilt somit ein Beweisverwertungsverbot.

8. KONTROLLRECHTE DES BETRIEBSRATES

Das Unternehmen verpflichtet sich, dem Betriebsrat im Sinne der §§ 89 und 91 ArbVG unaufgefordert über wesentliche Veränderungen bei Microsoft 365, die eine Anpassung dieser Vereinbarung zur Folge haben könnten, zu informieren.

Der Betriebsrat hat das Recht in sämtliche Protokolle, Ausdrucke und Auswertungen – unter Zugrundelegung der rechtlichen Anforderungen aus dem ArbVG – Einsicht zu nehmen. Zu diesem Zwecke hat das Unternehmen dem Betriebsrat einen Systemadministrator zur Verfügung zu stellen und den Betriebsrat mit den notwendigen Berechtigungen³ auszustatten

Zugang zu Hardware und Software ist ihm dabei zu gewähren.

Es ist dem Betriebsrat gestattet, externe Experten hinzuzuziehen, die vom Unternehmen bzw. den Fachabteilungen zu unterstützen sind. Diese Experten sind zur Verschwiegenheit verpflichtet.

Es ist dem Betriebsrat gestattet, an internen Schulungsmaßnahmen zu Microsoft 365 teilzunehmen.

9. RECHTE DER BESCHÄFTIGTEN

Alle Beschäftigten haben das Recht, eine allgemein verständliche Auflistung ihrer Daten einzufordern, Daten richtig zu stellen bzw. löschen zu lassen, wenn sie nicht berechtigt ermittelt wurden oder nicht richtig bzw. für den entsprechenden Zweck nicht mehr erforderlich sind.

3 Microsoft empfiehlt (<https://aka.ms/gutgemacht>, <https://tinyurl.com/2meus7bx>) für diese Zwecke die Berechtigung **Global Reader** (*Globaler Leser*)

10. ARBEITSGRUPPE MICROSOFT 365

Zur Evaluierung der Bestimmungen dieser Vereinbarung, zur Analyse der organisatorischen und technischen Veränderungen sowie als Anlaufstelle für betriebliche Erfahrungen im Umgang mit Microsoft 365 bilden Unternehmen und Betriebsrat eine prozessbegleitende Arbeitsgruppe Microsoft 365. Treffen finden zumindest zwei Mal pro Jahr statt.

Diese Arbeitsgruppe unterstützt das Unternehmen in seiner Rolle als datenschutzrechtlicher Verantwortlicher in der Ausarbeitung von transparenten Informationen an die von der Datenverarbeitung betroffenen Beschäftigten und berät diesen bei der Gestaltung von Schulungskonzepten.

Die Entscheidungskompetenzen der Unternehmensleitung als Organ des Unternehmens und die des Betriebsrates als Körperschaft gemäß ArbVG bleiben davon jedoch unberührt.

Die Anzahl der Teilnehmer wird zwischen Unternehmen und Betriebsrat vereinbart, wobei bei Bedarf auch externe Fachpersonen beigezogen werden können.

11. INKRAFTTRETEN

Diese Betriebsvereinbarung tritt mit xx.xx.20xx in Kraft und ist befristet bis zum xx.xx.20xx [jeweils 12 Monate]. Sollten in dieser Zeit keine Veränderungen im Umfang von Microsoft 365 eingetreten sein, die eine erweiterte Verarbeitung personenbezogener Daten möglich macht, verlängert sich diese Vereinbarung um weitere 12 Monate.

Ort, Datum

.....

für das Unternehmen

.....

für den Betriebsrat

BEILAGE: CHECKLISTE zum Einsatz von Microsoft 365

(vgl. <https://docs.microsoft.com/de-de/>)

- 1) **Wer sind die betriebsinternen Ansprechpersonen für Microsoft 365 und stehen für**
- technische,
 - organisatorische und
 - rechtliche
- Fragen zur Verfügung?**

- 2) **In welche Umgebung wird Microsoft 365 betrieben?**
- hybrid
 - cloud

- 3) **Welche Anforderungen der DSGVO/GDPR und des DSG wurden bisher erfüllt?**

datenschutzrechtliche Anforderung	j/n	Anmerkung
Rechenschaftspflicht nach Art 5 DSGVO/GDPR		
Verzeichnis von Verarbeitungstätigkeiten nach Art 30 DSGVO/GDPR		
Datensicherheitsmaßnahmen		
Transparenz gegenüber Betroffenen		
Datenschutz-Folgenabschätzung		

- 4) **Welche Verträge mit Auftragsverarbeitern wurden geschlossen und wo liegen diese auf?**

- 5) **Welches Microsoft 365 Lizenzmodell (Plan) ist in Verwendung?**

6) Welche der folgenden Komponenten/Services⁴ zu Office 365 sind im Einsatz?

	Komponente/n (Stand 03/2023)	j/n	Raum für Anmerkungen (Plan für Einführung), zusätzliche Anlage zur Betriebsvereinbarung
E3	Activity Report		
	Adoption Score		
	Alert Policies		
	Audio Conferencing (free add-on)		
	Audit		
	Azure AD for Office 365		
	Basis Mobility & Security		
	Bookings		
	Briefing Email		
	Compliance Manager		
	Data Loss Prevention		
	Delve		
	eDiscovery (standard)		
	Exchange Online Plan 2		
	Exchange Online Protection		
	InfoPath App		
	Information Protection for M365		
	Live Events		
	Message Encryption (basic)		
	Microsoft 365 Apps for Enterprise		
	Microsoft 365 Mobile App		
	Microsoft Dataverse for Teams		
	Microsoft Forms		
	Microsoft Lists		
	Microsoft Search		
	Microsoft Teams		
	Microsoft To Do		
	Microsoft Whiteboard		
	Office for the Web (incl Visio)		
	OneDrive for Business Plan 2		
	Planner		
	Power Apps for Office 365		
	Power Automate for Office 365		
	Power Virtual Agents for Teams		

4 Angelehnt an Darstellung von Aaron Dinnage „Microsoft 365 Enterprise“, siehe <https://m365maps.com/>

	Komponente/n (Stand 03/2023)	j/n	Raum für Anmerkungen (Plan für Einführung), zusätzliche Anlage zur Betriebsvereinbarung
E3	Productivity Server CAL		
	Project & Roadmap View Access		
	Retention Labels		
	Retention Policies		
	Secure Score		
	SharePoint Online Plan 2		
	Stream for Office 365		
	Sway		
	Viva Connections		
	Viva Engage		
	Viva Insights Personal (basic)		
	Viva Learning (basic)		
	Webinars		

	Komponente/n (Stand 03/2023)	j/n	Raum für Anmerkungen (Plan für Einführung), zusätzliche Anlage zur Betriebsvereinbarung
E5	Audio Conferencing (full)		
	Graph Connector Index Quota		
	Office 365 Cloud App Security		
	Power BI PRO		
	Skype for Business Plus CAL		
	Teams Phone		
	Viva Insights Personal (premium)		
	eDiscovery & Audit (E5 Compliance)		
	Insider Risk Management (E5 Compliance)		
	Information Protection & Governance (E5 Compliance)		
	Application Guard for Office (E5 Security)		
	Safe Documents (E5 Security)		
	Sentinel Benefit (E5 Security)		

7) Welche der folgenden Komponenten/Services des EMS (Enterprise Mobility + Security) sind im Einsatz?

	Komponente/n (Stand 03/2023)	j/n	Raum für Anmerkungen (Plan für Einführung), zusätzliche Anlage zur Betriebsvereinbarung
E3	Intune Plan 1 (Application Management, Config Manager, Device Management, Endpoint Analytics)		
	Active Directory RMS (Rights Management)		
	Azure RMS (Rights Management)		
	Config Manager Endpoint Protection		
	Endpoint Analytics		
	Information Protection		
	Windows Server CAL (Client Access Licenses) Rights		
	Azure Active Directory Premium Plan 1		
E5	Rules-Based Classification (Client & Scanner)		
	Defender for Cloud Apps		
	Defender for Identity		
	Azure AD Premium Plan 2 Step-up		

8) Welche der folgenden speziellen Features von Windows Enterprise werden verwendet?

	Feature (Stand 03/2023)	j/n	Raum für Anmerkungen (Plan für Einführung)
E3	Defender for Endpoint Plan 1		
	Always On VPN		
	Application Control		
	Application Guard		
	AppLocker		
	App Assure		
	Assigned Access		
	Attack Surface Reduction		
	Azure AD Join		
	BitLocker & BitLocker to Go		
	BranchCache		
	Cortana		
	Credential Guard		
	Custom Logon		

	Feature (Stand 03/2023)	j/n	Raum für Anmerkungen (Plan für Einführung)
E3	Custom Shell		
	Defender Antivirus		
	DirectAccess		
	Domain Join		
	Edge for Business		
	Keyboard Filter		
	Long Term Servicing Channel		
	Manage by MDM		
	Persistent Memory		
	Power Automate Attended Desktop Flows		
	Resilient File System (ReFS)		
	SMB Direct		
	Unbranded Boot		
	Unified Write Filter		
	Universal Print		
	Windows Autopatch		
	Windows Autopilot		
	Windows Conditional Access		
	Windows Firewall		
	Windows Hello for Business		
	Windows Update for Business		
	Windows Virtualization Rights		
	36 months support for Windows 11		
E5	Microsoft Defender for Endpoint Plan 2 Step-up (E5)		

9) Mit welchen Geräten (Devices) kann Microsoft 365 verwendet werden?

Geräte/Devices	j/n	Anmerkung
betrieblich ausgegebene und geprüfte Geräte (Devices)		
private Geräte, die geprüft wurden (BYOD)		
Geräte werden zusätzlich über Intune MDM verwaltet		

ANLAGEN

Die folgenden Anlagen konkretisieren Bestimmungen der „Betriebsvereinbarung über die Einführung und Anwendung von Microsoft 365“ zu ausgewählten Komponenten/Services/Apps im Hinblick auf

- technische
- organisatorische und
- rechtliche

Aspekte.

Übersicht

Nr.	Bezeichnung	Version (Stand)
1	Datenkategorien	
2	[Beispiel: Detailregelung zur Komponente A]	
3	[Beispiel: Detailregelung zur Komponente B]	

Anlage Nr. X (fortlaufende Nummerierung) zur

Betriebsvereinbarung über die Einführung und Anwendung von Microsoft 365

Diese Anlage ergänzt die Betriebsvereinbarung über die Einführung und Anwendung von Microsoft 365, indem spezifischere Regelungen für die/das folgende Komponente/Service/App definiert werden.

	Dokumentation
Bezeichnung Komponente/Service/App	*Text einfügen*
Zweck der Datenverarbeitung	*Text einfügen*
(optional) Nichtziel	*Text einfügen*
personenbezogene Daten	*Text einfügen*
vereinbarte personenbezogene Auswertungen und Analysen	*Text einfügen*
Übermittlung der erzeugten Daten in andere (Nicht-Microsoft-) Systeme (Beschreibung Schnittstelle)	*Text einfügen*
Übermittlung von Daten an betriebsexterne Empfänger	*Text einfügen*
Rollen- und Berechtigungskonzept	*Text einfügen*
(optional) organisatorische Regeln	*Text einfügen*
Anmerkungen	*Text einfügen*

Ort, Datum

.....

für das Unternehmen

.....

für den Betriebsrat