

# Betriebsvereinbarung zu Microsoft 365 (Eckpunkte)

## § 1 Gegenstand der Vereinbarung

- Genaue Bezeichnung der Software (Microsoft 365 Enterprise, ggf. mit Lizenztyp)
- In **Anlage 1** sind alle zulässigen bzw. freigegebenen Anwendungen von Microsoft 365 aufgeführt (wie Exchange Online, Sharepoint Online, Teams, OneDrive for Business, Planner, Forms, Delve etc.); alle anderen Anwendungen werden deaktiviert
- In **Anlage 1** sind auch zu vereinbaren:
  - Alle zulässigen bzw. freigegebenen Anwendungen/Komponenten aus dem Bereich Sicherheit und Compliance<sup>1</sup> wie Azure Active Directory, Azure Information Protection, Data Loss Prevention, Beweissicherungsverfahren, eDiscovery, Endpoint Manager (früher: Intune) etc.
  - Mit Hilfe von Microsoft 365 (z.B. über Sharepoint Online oder PowerApps) erstellte unternehmensspezifische Anwendungen, die Beschäftigtendaten verarbeiten
  - Externe bzw. verbundenen Anwendungen oder Dienste, die in Microsoft 365-Anwendungen (wie Teams) eingebunden werden und Beschäftigtendaten verarbeiten
- Soweit eine Betriebspartei dies verlangt, wird für eine in **Anlage 1** aufgeführte Anwendung von Microsoft 365 eine ergänzende Vereinbarung in **Anlage 2** abgeschlossen (z.B. Anlage 2.1 für Exchange Online, Anlage 2.2 für Sharepoint Online). Dabei ist zumindest zu regeln:
  - kurze, prägnante Beschreibung der Funktionalität,
  - Verarbeitung von Beschäftigtendaten (Zweckbestimmung, zulässige Kategorien von Beschäftigtendaten, zulässige Auswertungen von Beschäftigtendaten)
  - Vorgaben zur Nutzung im Unternehmen
  - Berechtigungskonzept
  - Fristen/Kriterien zur Löschung von Beschäftigtendaten

## § 2 Geltungsbereich

- Personell (alle Beschäftigten oder nur bestimmte Bereiche)
- Räumlich (→ Berücksichtigung mobiler Nutzung)

## § 3 Definitionen

- Relevante Begriffsdefinitionen von Microsoft 365
- Sonstige Begriffe gemäß den Definitionen in Art. 4 DSGVO

---

<sup>1</sup> Anwendungen, die i.d.R. für Administratoren aus dem *Security & Compliance Center* aufrufbar sind bzw. zum Bereich *Enterprise Mobility & Security* gehören

## § 4 Zulässige Verarbeitung von Beschäftigtendaten

- Beschäftigtendaten werden mit Microsoft 365 nur insoweit verarbeitet, wie dies durch diese Betriebsvereinbarung sowie die Anlagen zu dieser BV ausdrücklich zugelassen ist.
- Präzise Festlegung der Zwecke, zu denen Beschäftigtendaten mit Microsoft 365 verarbeitet werden dürfen:
  - Unterstützung der Kommunikation und Zusammenarbeit in Gruppen bzw. Teams
  - Umsetzung und Kontrolle von Datenschutz und IT-Sicherheit
  - Dokumentation des zuständigen Bearbeiters einer Aktivität zur Ermöglichung von Rückfragen, Klärung von Verantwortlichkeiten und Behebung von Fehlern im Einzelfall
  - Weitere zulässige Zwecke können in den ergänzenden Regelungen zu einzelnen Anwendungen von Microsoft 365 in **Anlage 2** festgelegt werden.
- Grundsatz der Datenminimierung
- Zulässige Kategorien von Beschäftigtendaten, die mit Microsoft 365 verarbeitet werden:
  - Personenbezogene Benutzerdaten, die übergreifend in verschiedenen M365-Anwendungen verarbeitet und mit Azure Active Directory synchronisiert werden, sind in **Anlage 3** dokumentiert.
  - Portraitbild für das Benutzerprofil: nur bei Einwilligung des betreffenden Beschäftigten,
  - Benutzerkennungen, Passwörter, Zugriffsrechte, Rollen,
  - Daten über Aktivitäten von Benutzern und Systemadministratoren in nach dieser BV zulässigen Protokolldateien bzw. Logfiles,
  - Bearbeiter eines Dokuments, eines Chats, eines Kommentars oder einer ähnlichen Aktivität (Benutzerkennung oder Name) mit Datum und Uhrzeit („Metadaten“),
  - weitere zulässige Kategorien von Beschäftigtendaten können in den ergänzenden Regelungen zu einzelnen Anwendungen von Microsoft 365 in **Anlage 2** festgelegt werden.
- Zulässige Verarbeitung von Beschäftigtendaten:
  - Nur zulässig, soweit dies zur Erfüllung der oben genannten zulässigen Zwecke erforderlich ist,
  - Auswertungen bzw. Reports von Beschäftigtendaten: nur soweit dies durch diese BV und ihre Anlagen ausdrücklich zugelassen sind.
  - Zulässige Auswertungen von Beschäftigtendaten können in den ergänzenden Regelungen zu einzelnen Anwendungen von Microsoft 365 in **Anlage 2** festgelegt werden.
  - Alle anderen möglichen, aber nicht zugelassenen Auswertungen sind soweit möglich technisch zu deaktivieren bzw. durch entsprechende Berechtigungsvergabe zu sperren.
- Die Nutzung der Aufzeichnungsmöglichkeiten von Bild- und/oder Tonaufnahmen in Microsoft 365 ist grundsätzlich untersagt und wird technisch unterbunden. Abweichend sind Aufzeichnungen zulässig, sofern dies für einzelne Microsoft 365-Anwendungen (wie z.B. Teams) ausdrücklich im Rahmen der **Anlage 2** näher geregelt wurde.

## § 5 Spezifische Microsoft 365-Regelungen

- Hier können bestimmte Funktionen von Microsoft 365 geregelt werden, als anwendungsübergreifende Regelungen, die mehrere Anwendungen von Microsoft 365 betreffen

- Aktivierung des Microsoft 365-Überwachungsprotokolls (*Audit Log*; Protokollierung aller Aktivitäten von Benutzer und Administratoren, auch bezüglich Änderungen von Konfigurations-Einstellungen, Berechtigungsvergabe etc.):
  - Nutzung des Überwachungsprotokolls nur zu Zwecken der Administration/Wartung sowie der Kontrolle von Datenschutz und IT-Sicherheit durch die dafür zuständigen Personen (nur diese erhalten Berechtigungen zur Nutzung des Überwachungsprotokolls bzw. der Audit Log Reports)
  - Speicherung nur für 90 bzw. 180 Tage (abhängig vom Lizenztyp)
  - Export und Speicherung der Daten aus Überwachungsprotokollen sind unzulässig (ggf. Ausnahme für Zweck der Kontrolle des Datenschutzes bzw. der Einhaltung dieser BV)
- Sog. Aktivitäten- und Nutzungsberichte (*Usage Reports, Activity Reports*) sind für Administrationszwecke für die jeweils zuständigen Administratoren zulässig, soweit sie nur zusammengefasste oder benutzerbezogene Daten über Nutzungshäufigkeiten und Ressourcenverbrauch für max. 180 Tage zurück enthalten. Abweichende Regelungen für einzelne Microsoft 365-Anwendungen gehen vor.
- Alle Aktivitäten- und Nutzungsberichte sind zu pseudonymisieren. Hierzu wird die entsprechende Funktion im globalen Admin-Center von M365 „Identifizierbare Benutzerinformationen in Berichten anzeigen“ deaktiviert. Statistische Auswertungen, die ausschließlich anonyme Bezeichnungen verwenden, können von den Administratoren weitergegeben werden.
- Berichte über erfolgreiche oder abgewiesene An- und Abmeldungen sind nur für Administrationszwecke zulässig
- Regelung zur Verfügbarkeitsanzeige (verfügbar, beschäftigt etc.): Freiwillige Nutzung durch jeden Benutzer; nur aktuelle Anzeige des jeweiligen Status, keine Aufzeichnung
- Regelungen zu Social Media-Funktionen (Kommentare, Bewertungen, Gefällt mir etc.)
- Regelungen bzgl. der Ablage nur für den Benutzer verfügbarer oder allgemein verfügbarer Dokumente (insbesondere in Sharepoint Online und OneDrive for Business): in welchen Fällen und zu welchen Zwecken?
- Nutzung von Microsoft 365-Anwendungen über mobile Endgeräte wie Smartphone, Tablets: nur wenn diese technisch abgesichert sind, z.B. über ein Mobile Device Management System, z.B. über Microsoft Endpoint Manager (früher: Intune), dann nach Vereinbarung einer ergänzenden Regelung in **Anlage 2** (zum Einsatz von Intune); Ausschluss privater Endgeräte
- Nutzung von Microsoft Graph und Delve:
  - Delve wird für alle Beschäftigten deaktiviert (ohne Möglichkeit der Aktivierung durch die Beschäftigten)
  - Delve wird erst nach ergänzender Vereinbarung in **Anlage 2** zur Nutzung freigegeben
  - Keine Nutzung von Microsoft Graph über die Graph-API-Schnittstelle
- Die Übertragung von Diagnose- oder Telemetrie-Daten an Microsoft wird seitens der Systemadministration deaktiviert bzw. - wenn dies nicht möglich ist - auf die Stufe mit der geringstmöglichen Datenübertragung an Microsoft eingestellt.

## § 6 Verknüpfung mit anderen Systemen, Schnittstellen

- Dokumentation aller Schnittstellen, über die Beschäftigtendaten von anderen IT-Systemen in Microsoft 365 gelangen oder von Microsoft 365 an andere IT-Systeme übergeben werden in **Anlage 4**

- Für jede Schnittstelle: Beschreibung der übergebenen Datenkategorien sowie des Zwecks der Verarbeitung in den anderen Systemen
- Zulässig ist die Schnittstelle zwischen dem Active Directory (AD) des Unternehmens und dem Azure Active Directory (AAD) von Microsoft 365. Im Rahmen der regelmäßigen Synchronisierung von AD und AAD werden die Datenarten gemäß **Anlage 3** zu Zwecken der Benutzer- und Berechtigungsverwaltung ausgetauscht.
- Regelung zum zulässigen Datenexport von Beschäftigtendaten in Excel o.ä. Software (oder ggf. Verbot des Exports)

## § 7 Aufbewahrungsfristen, Löschfristen

- Für alle Kategorien von Beschäftigtendaten sind konkrete Löschfristen bzw. Löschkriterien zu vereinbaren, unter Berücksichtigung gesetzlicher Aufbewahrungspflichten
- Festlegung der Löschfristen in dieser BV sowie in **Anlage 2** für spezifische Daten einzelner Microsoft 365-Anwendungen
- Soweit technisch möglich sind alle Löschfristen bzw. Löschkriterien automatisiert umzusetzen (über entsprechende Löschrichtlinien in Microsoft 365)
- Andernfalls sind weitere Vorgaben zur Umsetzung der Löschfristen bzw. Löschkriterien (z.B. Zuständigkeiten für Umsetzung und Überwachung) festzulegen

## § 8 Umsetzung des Datenschutzes

- Umsetzung und Dokumentation aller erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen (TOMs) gemäß Art. 32 DSGVO auf Basis einer Risikoanalyse bzw. Datenschutzfolgenabschätzung (DSFA);
  - Betriebsrat erhält die Dokumentation der TOMs und Ergebnis der DSFA (mit Stellungnahme des DSB) in Kopie
- Zugriffsberechtigungen für Microsoft 365 werden nur an Benutzer bzw. Administratoren vergeben, soweit es für die Erledigung ihrer regelmäßigen Arbeitsaufgaben erforderlich ist.
  - Alle übergeordneten Rollen, insbesondere Administrationsrollen, werden in **Anlage 5** dokumentiert.
  - Darüber hinaus gehende Berechtigungen für einzelne Microsoft 365-Anwendungen werden rollenbasiert in verständlicher und prüfbarer Form in **Anlage 2** festgelegt.
- Vorlage aller Verträge mit Auftragsverarbeitern gemäß Artikel 28 DSGVO (Software-Anbieter, Cloud-Anbieter, Wartungsunternehmen, Server-Betreiber etc.) gegenüber dem Betriebsrat
  - Alle relevanten Regelungen dieser BV sind bei den Verträgen zur Auftragsverarbeitung zu berücksichtigen
  - Nachweis ausreichender Garantien zur Umsetzung des Datenschutzes, sofern die Datenverarbeitung in Drittländern gemäß Art. 44 ff. DSGVO stattfindet
- Vertragliche Regelungen mit anderen Konzernunternehmen, die über Microsoft 365 Zugriff auf Beschäftigtendaten erhalten, zur Einhaltung der Regelungen dieser BV
- Möglichkeiten bzw. Notwendigkeiten zur Verschlüsselung personenbezogener Daten
- Systemadministratoren dürfen personenbezogene Daten, die sie im Rahmen ihrer Administrationaufgaben verarbeiten, nicht weitergeben; dies gilt auch im Verhältnis zu den Vorgesetzten

in den Fachbereichen. Unterweisung der Systemadministratoren bzgl. ihrer Pflichten nach dieser BV (nachvollziehbar dokumentiert)

- Arbeitgeber kontrolliert jährlich die Einhaltung dieser BV sowie der sonstigen geltenden Datenschutzvorschriften, insbesondere der TOMs (entsprechend Art. 32 Abs. 1 lit. d DSGVO); Prüfbericht in Kopie an den Betriebsrat, jeweils zum Stichtag .....; der Betriebsrat kann zu jeder jährlichen Prüfung eigene Prüffragen einreichen, die berücksichtigt werden müssen

## § 9 Leistungs- und Verhaltenskontrollen

- Leistungs- und Verhaltenskontrollen sind grundsätzlich unzulässig, soweit sie nicht durch diese BV ausdrücklich zugelassen sind:
  - Jeweils mit Benennung des konkreten Zwecks der Verarbeitung und der konkreten Kontrolle (oder deren Ausschluss)
  - Zulässig sind Kontrollen gemäß § 26 Abs. 1 Satz 2 BDSG (Straftaten im Beschäftigungsverhältnis), mit Konkretisierungen bzw. weiteren Anforderungen (rechtzeitige Information von BR und DSB, ggf. nur mit Zustimmung des BR; Möglichkeit zur Teilnahme von BR und DSB an der Kontrolle)

## § 10 Beweisverwertungsverbot

- Jegliche Verwertung von unzulässig verarbeiteten Beschäftigtendaten ausschließen, auch in arbeitsgerichtlichen Prozessen
- Unwirksamkeit von personellen Maßnahmen, die auf unzulässiger Verarbeitung von Beschäftigtendaten aufbauen

## § 11 Rechte des Betriebsrats

- Anlassbezogene und anlassunabhängige Kontrollrechte des Betriebsrats, direkt am System
  - Ggf. eigenständige Kontrolle des BR am System über „Global Reader“-Rolle, die dem BR zugewiesen wird
- Auskunftspflicht von kompetenten Mitarbeitern des Arbeitgebers gegenüber dem Betriebsrat
- Hinzuziehung von Sachverständigen nach § 80 Abs. 3 BetrVG zu Kontrollen des Betriebsrats
- Vetorecht des Betriebsrats bei unzulässigen Verarbeitungen von Beschäftigtendaten; betreffende Verarbeitungen werden deaktiviert (falls technisch möglich) oder durch andere geeignete Maßnahmen unterbunden
- Information des Betriebsrats über vom Arbeitgeber festgestellte unzulässigen Datenverarbeitungen mit Microsoft 365, ebenso bei Meldepflichten gemäß Art. 33, 34 DSGVO
- Möglichkeit zur geschützten Kommunikation des Betriebsrats (insbesondere Möglichkeiten zur Verschlüsselung der Dateiablage und der E-Mail-Kommunikation)

## § 12 Änderungen oder Erweiterungen

- Vorprüfung und Bewertung von Release-Notes und Roadmap von Microsoft, ob nur rein technische Änderungen (Fehlerkorrekturen, Usability-Verbesserungen oder Performance-Verbesserungen) vorliegen, durch den Arbeitgeber (mit geeigneter Archivierung, ggf. Mitteilung an BR)

- Widerspruchsrecht des Betriebsrats; falls wahrgenommen, Verhandlung zwischen Arbeitgeber und Betriebsrat
- Regelmäßige Information des BR über die wesentlichen Änderungen und Erweiterungen von Microsoft 365 entsprechend den Release-Notes und der Roadmap des Software-Herstellers; Beratung der Betriebsparteien hinsichtlich Mitbestimmung
- Soweit technisch möglich, werden Änderungen/Neuerungen in Microsoft 365 vor Umsetzung der Mitbestimmung nicht aktiviert bzw. keine Berechtigungen an neuen Anwendungen, Features, Reports etc. vergeben
- Änderungen oder Erweiterungen, die zu Abweichungen von den Vorgaben der BV und der Anlagen führen, insbesondere bzgl. der vereinbarten Anwendungen, Datenkategorien oder Auswertungen, des Berechtigungskonzepts sowie der technischen und organisatorischen Maßnahmen der Datensicherheit, unterliegen der Mitbestimmung des BR
- BR kann zusätzliche oder veränderte Regelungen zur BV verlangen, wenn sich seiner Meinung nach zusätzlicher Schutzbedarf für die Persönlichkeitsrechte der Beschäftigten ergibt (dann Verhandlungen der Parteien; falls keine Einigung: Einigungsstelle nach § 76 BetrVG)

### § 13 Schulungen, Qualifizierung

- Rechtzeitige und umfassende Qualifizierung über die Funktionen der eingesetzten Anwendungen von Microsoft 365, die Verwendung innerhalb der geplanten betrieblichen Einsatzszenarien
- Qualifizierung auch über die verfügbaren Datenschutz- und Sicherheitsfeatures von Microsoft 365, insbesondere zur Berechtigungssteuerung
- Rechtzeitige Planung der Qualifizierungsmaßnahmen: Übergabe eines Qualifizierungskonzepts an den zuständigen Betriebsrat (mit folgenden Inhalten: ...)
- Mitbestimmung des zuständigen BR bei den Qualifizierungsmaßnahmen

### § 14 Schlussbestimmungen

- Inkrafttreten, Kündigungsfristen, Nachwirkung
- Konfliktregelungen, Einigungsstelle
- Initiativrecht des Betriebsrats für Änderungen der BV oder zusätzliche Regelungen (z.B. bei Regelungslücken oder Verstößen gegen die BV), ohne Kündigung der gesamten BV; falls keine Einigung: Entscheidung durch Einigungsstelle