

Clara Fritsch

Die wunderbare Welt von Microsoft

Handlungsmöglichkeiten der Arbeitnehmer:innenvertretung

16

Praktische Gewerkschaftsarbeit



Die wunderbare Welt von Microsoft

Handlungsmöglichkeiten der
Arbeitnehmer:innenvertretung

Clara Fritsch

Die wunderbare Welt von Microsoft

Handlungsmöglichkeiten der
Arbeitnehmer:innenvertretung

Zeichenerklärung



Hinweise



Beispiele



Zitate

Die Inhalte in diesem Buch sind von der Autorin und vom Verlag sorgfältig erwogen und geprüft, dennoch kann eine Garantie nicht übernommen werden. Eine Haftung der Autorin bzw. des Verlages und seiner Beauftragten für Personen-, Sach- und Vermögensschäden ist ausgeschlossen.

Stand: Juli 2026

Impressum:

Layout/Grafik: Skripten-Team, ÖGB-Verlag

Medieninhaber: Verlag des ÖGB GmbH, Wien

© 2026 by Verlag des Österreichischen Gewerkschaftsbundes GmbH, Wien

Herstellung: Verlag des ÖGB GmbH, Wien

Verlags- und Herstellungsort: Wien

Druckerei: CITYPRESS GmbH, Neutorgasse 9, 1010 Wien

Printed in Austria

1 Vorwort	8
2 Was ist das Besondere an der Welt von MS 365?	10
3 Handlungsmöglichkeiten des Betriebsrates	18
3.1 Microsoft und die Arbeitsverfassung	18
3.2 Microsoft 365 und der Datenschutz	23
3.3 Microsoft 365 und die Künstliche Intelligenz (KI)	30
3.4 Microsoft 365 und der Gesundheitsschutz	32
4 Die Basis-Betriebsvereinbarung	38
4.1 Der Verwendungszweck oder die Zweckbindung	40
4.2 Das Berechtigungskonzept oder die Zugriffsbeschränkung	42
4.3 Die Speicherdauer	43
4.4 Die Privatnutzung	43
4.5 Das Profil	44
4.6 Das (angebliche) Fehlverhalten oder die Kontrolle	45
4.7 Die Schulung	46
4.8 Die Updates oder die Aktualisierung	48
4.9 Die Ansprechpartner:innen	50
5 Der Überblick und die einzelnen Anwendungen	52
5.1 Outlook (= E-Mail, Kalender, Kontakte)	56
5.2 Teams	59
5.3 Copilot und Agents – die KI bei MS 365	70
5.4 Anwendungen für IT-Administratorinnen und -Administratoren (Backend)	74

Inhalt

5.5 Graph	75
5.6 SharePoint	76
5.7 Purview und Defender	79
6 Nachwort	84
7 Anhang	86
8 Endnoten	90
Zur Autorin	91

SKRIPTEN ÜBERSICHT



SOZIALRECHT 	
SR-1	Grundbegriffe des Sozialrechts
SR-2	Sozialpolitik im internationalen Vergleich
SR-3	Sozialversicherung – Beitragsrecht
SR-4	Pensionsversicherung I: Allgemeiner Teil
SR-5	Pensionsversicherung II: Leistungsrecht
SR-6	Pensionsversicherung III: Pensionshöhe
SR-7	Krankenversicherung I: Allgemeiner Teil
SR-8	Krankenversicherung II: Leistungsrecht
SR-9	Unfallversicherung
SR-10	Arbeitslosenversicherung I: Allgemeiner Teil
SR-11	Arbeitslosenversicherung II: Leistungsrecht
SR-12	Insolvenz-Entgeltsicherung
SR-13	Finanzierung des Sozialstaates
SR-14	Pflege und Betreuung
Die einzelnen Skripten werden laufend aktualisiert.	

ARBEITSRECHT 	
AR-1	Kollektive Rechtsgestaltung
AR-2A	Betriebliche Interessenvertretung
AR-2B	Mitbestimmungsrechte des Betriebsrates
AR-2C	Rechtstellung des Betriebsrates
AR-3	Arbeitsvertrag
AR-4	Arbeitszeit
AR-5	Urlaubsrecht
AR-6	Entgeltfortzahlung im Krankheitsfall
AR-7	Gleichbehandlung im Arbeitsrecht
AR-8A	ArbeitnehmerInnenschutz I: Überbetrieblicher ArbeitnehmerInnenschutz
AR-8B	ArbeitnehmerInnenschutz II: Innerbetrieblicher ArbeitnehmerInnenschutz
AR-9	Beendigung des Arbeitsverhältnisses
AR-10	Arbeitskräfteüberlassung
AR-11	Betriebsvereinbarung
AR-12	Lohn(Gehalts)exekution
AR-13	Berufsausbildung
AR-14	Wichtiges aus dem Angestelltenrecht
AR-15	Betriebspensionsrecht I
AR-16	Betriebspensionsrecht II
AR-18	Abfertigung neu
AR-19	Betriebsrat – Personalvertretung Rechte und Pflichten
AR-21	Atypische Beschäftigung
AR-22	Die Behindertenvertrauenspersonen

GEWERKSCHAFTSKUNDE 	
GK-1	Was sind Gewerkschaften? Struktur und Aufbau der österreichischen Gewerkschaftsbewegung
GK-2	Geschichte der österreichischen Gewerkschaftsbewegung von den Anfängen bis 1945
GK-3	Die Geschichte der österreichischen Gewerkschaftsbewegung von 1945 bis heute
GK-4	Statuten und Geschäftsordnung des ÖGB
GK-5	Vom 1. bis zum 19. Bundeskongress
GK-7	Die Kammern für Arbeiter und Angestellte
GK-8	Die sozialpolitischen Errungenschaften des ÖGB
GK-9	Geschichte der Kollektivverträge

Die VÖGB-Skripten online lesen oder als Gewerkschaftsmitglied gratis bestellen:
www.voegb.at/skripten

1 Vorwort

Microsoft (MS) ist in den 1980er-Jahren mit einem Betriebssystem groß geworden und somit das älteste Unternehmen unter den Big Tech, zu denen Alphabet (Google), Amazon und Meta zählen. Microsoft zeichnet sich unter diesen Firmen nicht nur durch sein langes Bestehen, sondern auch durch sein ausgesprochen breites Angebot aus. Neben der Bürosoftware „Office“ und dem Betriebssystem „Windows“ bietet Microsoft vieles mehr, wie zum Beispiel die Sicherheits- oder Überwachungssoftware „Purview“ und „Sentinel“, eine Suchmaschine namens „Bing“, einen Browser namens „Edge“, diverse Kommunikationssysteme wie „Teams“ oder „Outlook“ oder das 2023 ins Leben gerufene System „Copilot“, das mit Künstlicher Intelligenz (KI) arbeitet und auf der Software von OpenAI basiert. Alles zusammen ist in dem Paket „Microsoft 365“ enthalten.

Software von Microsoft (MS) wird an fast allen Arbeitsplätzen verwendet. Ob privat oder im Betrieb, im Büro oder in der Fabrik, Microsoft bewältigt sämtliche Aufgaben des täglichen Arbeitslebens – wenn es so gewünscht wird. Die Arbeitnehmer:innen sind den Umgang mit MS-Produkten gewohnt.

Laufend werden Produkte neu erfunden, geändert, ergänzt, umbenannt, Funktionen anders zugeordnet, Einstellungen umgestaltet ... MS passt beispielsweise seine Vertragsklauseln an (neue) Gesetzesvorgaben an. MS trennt beispielsweise im April 2024 die Plattform „Teams“ von MS 365, nachdem die EU-Kommission ein Verfahren wegen Verletzung des Wettbewerbsrechts eingeleitet hatte. MS 365 und seine zahlreichen Anwendungen liegen in der Regel auf Servern von Microsoft, also „in der Cloud“. MS agiert also rasch und flexibel, sowohl in technischer als auch in juristischer Hinsicht.

Damit wird eine Vielzahl von Fragen aufgeworfen:

- Wer kann die Produktpalette von MS 365 überblicken und **kritisch begutachten**?
- Wie hängen die Angebote von MS 365 miteinander zusammen und was wird zu welchem **Zweck** verwendet?
- Werden die Beschäftigten mittels MS 365 bei der Arbeit **unterstützt oder überwacht**?

- Wie kann sich ein **Betriebsrat (BR) einbringen**? Benötigt die Interessenvertretung der Arbeitnehmer:innen ein eigenes Wörterbuch, um MS 365 zu verstehen? Falls eine Antwort auf diese Frage gesucht wird, findet ihr sie im Anhang in unserem „kleinen Wörterbuch“.
- Kann **MS 365 in einer Betriebsvereinbarung (BV)** geregelt werden?

→ **In diesem Skriptum wird diesen Fragen nachgegangen, um eine effektive Interessenvertretung für Arbeitnehmer:innen zu ermöglichen.**

Klar ist bei diesem Skriptum, dass es nie vollständig, geschweige denn abgeschlossen sein wird – dazu ist MS 365 zu variantenreich und zu schnelllebig. Was möglich ist, ist, Ansatzpunkte für den Umgang mit MS 365 zu liefern sowie Regelungen für die Mitsprache der Arbeitnehmer:innenvertretung aufzuzeigen.

→ **Betriebsrätinnen und Betriebsräte werden hier über die Software von MS 365 allgemein informiert und dabei unterstützt, eine Betriebsvereinbarung abzuschließen.**

Die ersten Kapitel geben einen Einblick in die Welt von Microsoft. Danach beschäftigt sich das Skriptum mit den arbeits- und datenschutzrechtlichen Aspekten. Die nach langjähriger Beratungserfahrung in der Gewerkschaft GPA am meisten eingesetzten sowie die heikelsten Anwendungen von MS 365 werden im Kapitel „Der Überblick und die einzelnen Anwendungen“ skizziert.

Was ist das Besondere an der Welt von MS 365?

Microsoft wurde 1975 gegründet, hatte also 2025 seinen 50. „Geburtstag“ gefeiert. Das ist für ein Technologieunternehmen, das zu den größten der Welt zählt, ein beachtliches Alter, gemessen an den anderen großen Playern Alphabet, Amazon, Apple und Meta, die bei ihren Gründungsdaten auf die 1990er- bzw. 2000er-Jahre zurückblicken. Trotz einiger weniger gelungener Produkte (wie beispielsweise dem „Windows Phone“, mit dem sich MS auf dem Handymarkt zu etablieren versuchte, dem Browser „Explorer“, der mit Sicherheitsmängeln zu kämpfen hatte und schließlich unterging, oder dem Versuch, eine Streaming-Plattform namens „Mixer“ ins Leben zu rufen) zählt MS zweifelsfrei zu den Riesen der Techbranche.

Der Konzern Microsoft bietet das weltweit meistgenutzte Betriebssystem „Windows“ an. Das Unternehmen dürfte ebenso Marktführer bei Bürosoftware sein – genaue Verkaufszahlen gibt es weder für Europa noch für den deutschsprachigen Raum, geschweige denn für Österreich. Bekannt ist, dass der deutsche Bund 2025 500 Millionen Euro für Lizenzen bezahlt hat.¹ Microsoft hat somit einen Monopolstatus.

Bürosoftware namens MS 365 (ehemals „Office 365“) ist seit Oktober 2010 auf dem Markt und umfasst ein ausgesprochen breites Spektrum. MS 365 kann eingesetzt werden zur **Kommunikation, Zusammenarbeit, Datenanalyse, technischen Sicherheit** (Cybersecurity), **Finanzplanung, Projektplanung, Gerätemanagement, Personalmanagement** u. v. m.

Die meisten Ressourcen steckt Microsoft derzeit in den Ausbau der sogenannten **Copilot**-Anwendungen, das sind jene, die mit Künstlicher Intelligenz (KI) arbeiten. Aus *einem* Copilot sind seit 2022, also in nur drei Jahren, über 80 (verschiedene) geworden, die jeweils mit KI arbeiten und unterschiedliche Abläufe weitgehend „selbstständig“ ausführen können. Diese sogenannten **Agents** (Seite 70), bestehend aus miteinander gekoppelten Ausführungsschritten, sind momentan der „letzte Schrei“ auf dem Marktplatz von MS 365.

In den letzten fünf Jahren hat MS außerdem folgende Plattformen stark ausgebaut:

- **Power Platform:** Das sind Anwendungen, die betriebsintern maßgeschneidert werden
- **Teams:** Das von einem Videokonferenztool zu einer eigenen Plattform ausgebaut worden ist, auf der neben Videokonferenzen, Online-Zusammenarbeit und Dateimanagement ebenso stattfinden können, wie Terminkoordination, Aufgabenplanung, Aktivitätsübersichten oder persönliche Unterhaltungen. Je nach Bedarf können weitere Anwendungen eingehängt werden.
- **Viva:** Besteht (derzeit) aus unterschiedlichsten Anwendungen, bei denen es vorrangig um das Verhalten von Nutzerinnen und Nutzern geht. Viva ist es deshalb wert, sich damit etwas näher auseinanderzusetzen, weil es ein typisches Beispiel für die Vorgehensweise von MS ist – ein Produkt wird umbenannt, auf mehrere aufgeteilt, die kritische Verhaltensanalyse verschoben und somit „versteckt“. Die heftig kritisierten Auswertungsmöglichkeiten des Verhaltens von Beschäftigten mittels „Workplace Analytics“, für das Microsoft 2021 den Negativpreis „**Big-Brother-Award**“ erhielt, tauchen 2021 in „Viva Insights“ wieder auf. Vieles, was heute „Viva“ heißt, lief bis 2020 unter dem Namen „Workplace Analytics“ und bot Führungskräften großzügig Einsicht in das Verhalten von Nutzerinnen und Nutzern.² Bei Viva wurde eine vormals eher nebensächliche Anwendung, die 2021 ins Leben gerufene „Viva Connections“, in viele Teile aufgeteilt und Analysen aus Anwendungen übernommen, von denen einige Datenmaterial mit übermäßigem Kontrollcharakter liefern. Derzeit laufen Viva-Anwendungen unter den Namen:
 - **Viva Engage** (eine Art Schwarzes Brett für Wissensaustausch und Selbstdarstellung),
 - **Viva Connections** (eine Art Intranet für Einzelne oder Teams),
 - **Viva Learning** (Plattform zur Abwicklung von Weiterbildungsangeboten),
 - **Viva Sales** (zum Kundinnen- und Kundenmanagement),
 - **Viva Goals** (eine Übersicht und Verwaltung für Zielvereinbarungen),
 - **Viva Amplify** (zur Verwaltung von mehreren gleichzeitig laufenden Kommunikationskanälen für Marketing),
 - **Viva Pulse** (Umfragetool für Führungskräfte für anonyme Feedbacks und Stimmungsmessung unter den Beschäftigten),

Was ist das Besondere an der Welt von MS 365?

- **Viva Glint** (für die intensive Auseinandersetzung mit der Meinung der Beschäftigten sowie Maßnahmen, die darauf aufbauen³),
- **Viva Insights** (Darstellung persönlicher Verhaltensmuster).

→ **Viva-Anwendungen ermöglichen meist eine umfassende – und mitunter fragwürdige – Auswertung von Telemetrie- bzw. Verhaltensdaten der Nutzer:innen. Der Betriebsrat sollte sich gut überlegen, welche der Anwendungen für welche Zwecke geeignet sind und in einer Betriebsvereinbarung geregelt werden sollten.**

MS 365 hat auf allen Organisationsebenen etwas zu bieten. Es gibt Software, die für ein gesamtes Unternehmen von Bedeutung ist (z. B. die Plattform SharePoint oder der „Türsteher“ Defender). Für das Management auf der Ebene von Gruppen, Bereichen, Abteilungen oder Niederlassungen hat MS 365 auch ein großes Angebot (z. B. die Plattform Teams (Seite 59) oder MS Dynamics, eine Plattform zur Personalverwaltung). Und schließlich gibt es für die einzelnen Nutzer:innen jede Menge Anwendungen, sowohl zur Zusammenarbeit mit anderen (z. B. Outlook [Seite 56]) als auch zur Organisation der persönlichen Arbeit (z. B. OneDrive).

Diese verschiedenen Ebenen sind über „**Graph**“ (Seite 75) miteinander verbunden. Alle Anwendungen, alle Nutzer:innenaktivitäten, Zugriffe, Berechtigungskonzepte, alle Einstellungen, sämtliche Berechnungen, Tätigkeiten und Prozesse, also das gesamte „Microsoft-Universum“ und ebenso alle mit MS 365 verbundenen Systeme werden über die „**Super-Schnittstelle Graph**“ verarbeitet. MS 365 beinhaltet zusätzlich zu den eigenen, miteinander verflochtenen Anwendungen Möglichkeiten zur Einbindung externer Software. Es können beliebige **Erweiterungen** eingebunden werden (beispielsweise aus anderen Welten wie Google, Cisco Webex oder Zoom).

Die Anwendungen von MS 365 werden permanent verändert, ausgebaut, adaptiert, untereinander kombiniert, an Sicherheitserfordernisse angepasst. Anwendungen werden neu erfunden, neu eingeführt, sie werden „ausgerollt“ oder in bestehende „Apps“ integriert.



Hier einige größere Beispiele für die ununterbrochen anhaltenden Veränderungen in der Welt von MS 365.⁴

- Die Videotelefonie mittels „**Skype**“ wird seit 2021 nicht mehr angeboten und ist in die Videotelefonie von Teams übergegangen;
- früher **Yammer**, eine Austauschplattform, wurde 2017 von MS übernommen und schrittweise in das eigene Angebot aufgenommen, 2023 eingestellt und ist nun gänzlich in „**Viva Engage**“ aufgegangen;
- Security-Apps zum Management von Identität und Authentifizierung werden seit 2023 unter dem Namen „**Entra**“ zusammengefasst;
- die automatische **Standorterfassung** (engl.: Tracking) im firmeninternen WLAN über Teams „**Places**“ (Seite 67) wurde aufgrund massiver öffentlich geäußelter Bedenken vorerst von Jänner auf April 2026 verschoben und schließlich im August 2026 inklusive einer etwas privatsphärefreundlicheren Einstellung ermöglicht.

MS 365 enthält Funktionen, die **quer über verschiedene Anwendungen** aktiv sind. Sie sind quasi „**Meta-Anwendungen**“ (z. B. Standort, Status, Sprachsteuerung). Beispielsweise kann die Spracherkennung in einem Word-Dokument im Sinne eines Diktiergeräts zum Einsatz kommen, sie kann für das Transkribieren von Teams-Sitzungen verwendet werden oder auch ein Befehl in Power BI zum Auswerten einer Excel-Tabelle sein.

Die Server von MS 365 können an unterschiedlichen Standorten betrieben werden. MS 365 kann auf firmeneigenen Servern laufen (die Bezeichnung dafür lautet „on-premise“) oder die Anwendungen werden aus der **Cloud** heruntergeladen. Es kann damit gänzlich auf eigene Server verzichtet und auf den MS-eigenen Servern gearbeitet werden – also in der Cloud installiert, gewartet, repariert, ausgetauscht, ergänzt etc. Personal, Speicher- und Rechnerkapazitäten sowie IT-Know-how werden damit von MS zur Verfügung gestellt. IT-Verantwortliche berichten aus der Praxis, dass ihre Ressourcen dennoch stark gefragt sind, da das betriebsspezifische Einrichten, das Erstellen von Richtlinien, das Aufklären der

Was ist das Besondere an der Welt von MS 365?

Belegschaft und das Verfolgen der permanenten Updates einen zumindest ebenso großen Aufwand darstellen wie die IT-Arbeit ohne MS-Anwendungen.

Die MS Server sind über unterschiedliche **Standorte** verstreut. In Europa liegen die großen Serverfarmen derzeit in Amsterdam, Dublin, Frankfurt, Berlin, Magdeburg, Mailand, Zürich, Genf, London, Cardiff, Madrid, Oslo, Stavanger, Warschau, Budapest und Bukarest. In Wien-Gerasdorf wurde 2025 ein neues Rechenzentrum errichtet. Jedes der Rechenzentren hat einen „Zwilling“, um bei Ausfällen sofort ausweichen zu können und so die Kapazitäten zu erhalten.

→ **Damit die Daten einer Firma in Europa verarbeitet werden, empfiehlt es sich, gleich zu Beginn der Migration auf MS 365 die sogenannte „Local Residency-Richtlinie“ festzulegen, was die Datenhaltung im EU-Raum am jeweils gewünschten Ort ermöglicht. Administratorinnen und Administratoren können das in der Azure Global-Infrastructure einrichten.**

Die Verfügbarkeit und **Stabilität** dürften bei MS 365 sehr verlässlich sein. Sollten MS-Anwendungen dennoch einmal versagen, hat das jedoch gravierende Auswirkungen, wie im Juli 2024 der Update-Fehler des bei MS 365 für die Security zuständigen Betreibers CrowdStrike zeigte. Dadurch waren weltweit Krankenhäuser, Flughäfen und andere wichtige Einrichtungen lahmgelegt. Zwar investiert MS in einem Ausmaß in die technische Sicherheit und Gefahrenabwehr (engl. „safety and security“), das einzelnen Unternehmen im Regelfall nicht zur Verfügung steht, jedoch sind Sicherheitslücken, wenn sie auftreten, aufgrund der weiten Verbreitung von MS immens.

Interpretation von Beschäftigtendaten: Was macht MS 365 mit unseren Daten?

MS 365 bietet eine riesige Menge an Anwendungen und in jeder Anwendung verschiedene Einstellungen. Alle Anwendungen sind im Hintergrund miteinander über Graph verknüpft. Jede Anwendung erzeugt im Hintergrund Verbindungs- und Verhaltensdaten (auch Metadaten oder Telemetriedaten genannt). MS 365 übermittelt die Telemetriedaten (das sind Diagnosedaten wie z. B. das letzte Softwareupdate, Fehlerdokumentation, Verbindungsdauer, Geschwindigkeit der

Übermittlung, Datenschutzeinstellungen etc.) an MS. Das hat den Nebeneffekt, dass sämtliche Metadaten von MS interpretiert werden können. MS kann damit Vergleiche anstellen, Schwellenwerte erzeugen (englisch: „Benchmarks“) und auf deren Basis Anwendungen „optimieren“. Egal, ob privatsphärefreundliche Einstellungen (engl. Privacy by default) selbstständig deaktiviert wurden oder nicht, laufen Aufzeichnungen des Nutzer:innenverhaltens im Hintergrund mit und sind somit vorhanden. MS 365 ist in der Cloud permanent online und übermittelt ununterbrochen Daten an Microsoft.

Dieser Datenschatz aus einer gigantischen Menge an Metadaten und die daraus gezogenen Innovationen sind es, die MS groß gemacht haben.

Bei den vorhandenen Metadaten handelt es sich nicht nur um die Nutzungsdaten Einzelner (z. B. deren individuelle Vorlieben bei Privatsphäre-Einstellungen, deren persönliche E-Mail-Öffnungsraten, bevorzugte Nutzungszeiten etc.), sondern auch um die Beziehungen der einzelnen Nutzer:innen untereinander (z. B. durchschnittliche Reaktionsgeschwindigkeit auf bestimmte Kontaktpersonen, häufige Kommunikationspartner:innen, Vergleiche innerhalb einer Gruppe etc.). So kann nicht nur zu jeder Nutzerin und zu jedem Nutzer, sondern auch zu jeder Gruppe, jedem Team, jeder Abteilung ein vergleichendes Profil zusammengestellt werden.



Beispiele für Interpretationen:

- Haben Nutzer:innen **Terminkollisionen** in ihren Kalendern, geht man in der MS-Logik von „abgelenkten Teilnehmerinnen und Teilnehmern“ aus. Es könnte aber schlicht daran liegen, dass ein abgesagter Termin nicht gelöscht wurde.
- Sind einem Termin keine weiteren Teilnehmer:innen zugeordnet, wird dieser als mögliche „**Fokuszeit**“ angezeigt, also um konzentriert zu arbeiten. Um die beste Fokuszeit festzulegen, wird ausgewertet, wie „aktiv“ jemand in den MS Anwendungen ist. MS schlägt somit auch wenig hilfreiche „Fokuszeiten“ vor, bei denen es sich um ein Webinar mit Teilnehmenden außerhalb der über Outlook bekannten Kontakte handelt oder etwa um einen Arzttermin.

Was ist das Besondere an der Welt von MS 365?



- Bestehen viele **Interaktionen mit Personen** aus den MS-Kontakten (z. B. gemeinsame Termine, gemeinsam bearbeitete Projekte, geteilte Dokumente auf OneDrive etc.), wird dieser Umstand positiv beurteilt. Kolleginnen oder Kollegen mit hohem Vernetzungsgrad werden von MS als „erfolgreich“ bewertet (z. B. in Viva Goals, Viva Glint, Usage Analytics in Power BI, Copilot Teams). In der beruflichen Praxis sagen die Menge und Größe an E-Mails nicht unbedingt etwas über deren Qualität aus; viele unklar formulierte E-Mails sind nicht besser als eine verständliche.
- Es können Gruppen und deren **Meetings analysiert** werden. Wer ein Meeting in Teams festsetzt, kann auch dessen Analyse starten (z. B. Beteiligung in Form von Chats oder Wortmeldungen, Pünktlichkeit, Anzahl hochgeladener Dateien ...) – auch ohne Wissen oder Zustimmung der oder des Einzelnen (z. B. mittels Power BI oder Viva Glint).
- „Viva Insight“ berechnet, wann die individuell besten Zeitfenster für „**well-being**“ (deutsch: Wohlbefinden) bestehen, wobei freie Zeitfenster im Kalender angezeigt werden, genauere Berechnungsgrundlagen jedoch im Dunkeln bleiben. Viva Insight gibt Tipps wie „Deaktivieren Sie Arbeit außerhalb der Arbeitszeit“, wobei alles, was außerhalb der MS-Anwendungen geschieht, nicht als Arbeitszeit gilt.

MS 365 errechnet also Zusammenhänge, die nicht unbedingt sinnvoll sind, und trifft damit Aussagen über Sozialverhalten oder zeiteffizientes Verhalten. Nachdem die Rechenmodelle im Hintergrund aber nicht offengelegt werden, ist nicht ersichtlich, ob die Grundannahmen sinnvoll sind. Genauso unklar bleibt, ob ethische Grundprinzipien einfließen und rechtliche Vorgaben eingehalten werden (z. B. dass Entscheidungen aufgrund von maschinellen Berechnungen jederzeit widerrufbar sein müssen, dass Pausen eingehalten werden müssen etc.). Ebenso unklar ist, ob die Berechnungen wissenschaftliche Grundprinzipien der Mathematik und Statistik einhalten. Ohne die Berechnungsgrundlagen zu kennen, sind Empfehlungen von MS 365 wenig gehaltvoll. Sicher wird – schon allein aufgrund

der massenhaft vorhandenen Daten – der eine oder andere „Treffer“ zustande kommen, aber die Frage nach dessen Nutzen für die tägliche Arbeit bleibt offen.

- **Der Betriebsrat kann sich eine Übersicht über die Telemetriedaten verschaffen, indem er sich über die Windows-App „Diagnosedatenanzeige“ ansieht, welche Diagnosedaten von Office erhoben und übermittelt werden. Inwieweit es sinnvoll ist, die Telemetriedaten abzuschalten, muss mit der IT-Abteilung geklärt werden, da es zu Problemen mit IT-Support durch Microsoft bzw. mit Windows-Updates kommen kann.**



MS 365 ermittelt laufend Telemetriedaten über den Systemzustand und Nutzer:innenaktivitäten. Dies kann technisch nicht ausgeschlossen werden. Seitens der lokalen Systemadministratorinnen und -administratoren ist sicherzustellen, dass diese Daten nur für das Beheben von Fehlern, Sicherheits- oder Auslastungsproblemen verwendet werden, nicht jedoch zur Leistungsfeststellung oder zum Leistungsvergleich einzelner Nutzer:innen.

- **Admins können über sog. Gruppenrichtlinien einstellen, ob und in welchem Umfang Diagnosedaten erfasst und an Microsoft übermittelt werden (z. B. über lokale Firewall, Deaktivierung der Telemetrie auf dem Windows Server, Deaktivierung von Telemetrie-Dienst und dazugehörigem „Event Tracing for Windows Autologger“). Somit können die lokalen Systemadministratorinnen und -administratoren sicherstellen, dass keine Benutzer-ID, Betreffzeilen oder Inhaltsdaten in den an MS übermittelten Telemetriedaten enthalten sind.**

Handlungsmöglichkeiten des Betriebsrates

3

Aus dem Arbeitsverfassungsgesetz (ArbVG), dem ArbeitnehmerInnenschutzgesetz (ASchG) und der Europäischen Datenschutz-Grundverordnung (DSGVO) sowie beim Einsatz von KI-Anwendungen auch aus der KI-Verordnung ergeben sich Möglichkeiten, wie sich Betriebsrätinnen und Betriebsräte bei der Gestaltung von MS 365 einbringen können.

3.1 Microsoft und die Arbeitsverfassung

Allgemeines Überwachungsrecht (§ 89 ArbVG): Betriebsrätinnen und Betriebsräte können sich darauf berufen, dass sie die Einhaltung von gesetzlichen Vorgaben überwachen müssen (z. B. indem sie Einsicht nehmen). Dazu gibt es bei MS 365 verschiedene praktische Möglichkeiten. Beispielsweise kann eine eigene „Rolle“, also eine Leseberechtigung, für die Betriebsrätin und den Betriebsrat eingerichtet werden. Es könnte auch eine MS 365-Datenschutzgruppe mit regelmäßigen Informationstreffen ins Leben gerufen werden. Oder der BR fordert fixe Abläufe zur Informationsweitergabe ein, damit das Überwachungsrecht gewahrt ist.

Interventions- und Beratungsrecht (§ 92 ArbVG): Betriebsratsmitglieder sind dazu berechtigt, angehört zuwerden, wenn sie ihre Meinung, ihre Beobachtungen, ihre Wünsche vorbringen wollen. Bei Treffen im Rahmen des Beratungsrechts können sie etwa berichten, welche (gesundheitlichen) Auswirkungen zu MS 365 sie im Betrieb feststellen, sie können Vorschläge zur Gestaltung oder Deaktivierung einzelner Anwendungen vorbringen. Diese Anhörung muss gegeben sein. „Reds in ein Sackerl und stells vor die Tür“ ist keine rechtskonforme Vorgehensweise.

Informationsrecht (§ 92 ArbVG): Betriebsratsmitglieder können eine umfassende Information verlangen (z. B. welche Anwendungen in Betrieb sind, wer Einsicht nehmen kann, welche Daten personenbezogen ausgewertet werden, wo Daten gespeichert werden etc.).

Mitwirkungsrechte (§ 96 ff. ArbVG): Das österreichische Arbeitsverfassungsgesetz (ArbVG) sieht in diversen Fällen die Mitwirkung des Betriebsrats vor. Die für den BR stärkste Bestimmung im Zusammenhang mit Kontrollsystemen – und als solches kann MS 365 mit seiner Fülle an Aufzeichnungsmöglichkeiten bezeichnet

Microsoft und die Arbeitsverfassung 3.1

werden – gibt vor, dass „die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer:innen, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren“ (§ 96 Abs. 1 Z 3 ArbVG), der Zustimmung des Betriebsrates bedürfen. Man spricht von einer „**notwendigen Betriebsvereinbarung**“. Durch das Zusammenspiel der verschiedenen MS 365-Anwendungen untereinander ist das System geeignet, Arbeitnehmer:innen zu kontrollieren.

→ **Angesichts der lückenlosen Aufzeichnung des Nutzungsverhaltens ist eine Betriebsvereinbarung gemäß § 96 Abs. 1 Z 3 ArbVG abzuschließen.**

Das Erfassen von Verbindungsdaten, Standortdaten, Präsenzstatusangaben, der zeitlichen Dauer von Interaktionen etc. sind zahlreiche Möglichkeiten zur Kontrolle von Arbeitnehmerinnen und Arbeitnehmern. Diese umfangreichen Datensammlungen von MS 365 sind mit an Sicherheit grenzender Wahrscheinlichkeit allein schon durch ihre Vielzahl und ihr stetes Vorhandensein eine Kontrollmaßnahme.

Es kommt bei der „**Kontrollmaßnahme**“ im Sinne des ArbVG nicht auf eine subjektive Absicht zur Überwachung durch Vorgesetzte, andere Kolleginnen, Kollegen oder die bzw. den Arbeitgeber:in selbst an, sondern auf die *objektive Eignung* der Maßnahme bzw. des Systems zur Kontrolle. Die bloße Möglichkeit zur Kontrolle reicht aus, damit ein System zustimmungspflichtig ist. Ein österreichisches Arbeitsgericht hat dazu zwar (noch) keine Rechtsprechung abgegeben, doch liegt das daran, dass es vor einer solchen Rechtsprechung (bislang) immer zu einer Einigung in Form einer Betriebsvereinbarung gekommen ist.

Von einem „Berühren der **Menschenwürde**“ sprechen Juristinnen und Juristen dann, wenn bei den überwachten Personen das Gefühl einer dauerhaften Überwachung entsteht, die Kontrolle also über das für die Arbeitserbringung nötige Maß hinausgeht. Durch die Rechtsprechung haben sich folgende Kriterien herausgebildet, die bei der Frage, ob die Menschenwürde berührt ist, eine Rolle spielen:

Handlungsmöglichkeiten des Betriebsrates

1. Je häufiger die Kontrollmaßnahme gesetzt wird, desto stärker ist die Menschenwürde berührt (**Kontrolldichte**); wird einmal im Jahr kontrolliert? Einmal im Quartal? Täglich? Oder wird jede einzelne Tätigkeit im gesamten Arbeitsverlauf mitverfolgt – bei Letzterem ist die Menschenwürde sicher berührt. Nachdem durch MS 365 üblicherweise sehr viele Arbeitsprozesse erfasst sind oder zumindest erfasst sein können, könnte eine lückenlose Aufzeichnung der Tätigkeiten von Arbeitnehmerinnen und Arbeitnehmern erfolgen und die Menschenwürde ist somit berührt.
2. Je weiter die Kontrollmaßnahme in den Privatbereich hineinreicht, desto stärker ist die Menschenwürde berührt (**Kontrollintensität**); wird ein Kundengespräch aufgezeichnet oder wird ein Privatgespräch aufgezeichnet? Wird ein (Video-)Meeting im Büro oder im Homeoffice mitverfolgt? Wird der Weg zu einer Klientin oder einem Klienten getrackt oder der Weg auf die Toilette? – bei Letzterem ist die Menschenwürde nicht nur berührt, sondern verletzt und es ist somit untersagt.
3. Je nachdem, worauf eine Kontrollmaßnahme beruht, auf welche Art und Weise sie ausgeübt werden kann, kann die Menschenwürde berührt sein (**objektive Eignung**). Es muss also beachtet werden, was konkret im Betrieb im Einsatz ist. Betriebsratsmitglieder, die eine Betriebsvereinbarung durchsetzen möchten, müssen erklären können, worin die Kontrollmaßnahme konkret besteht. Die reine Behauptung, dass Arbeitgeber:innen Kontrolle ausüben, wird nicht ausreichen, um von der Eigenschaft als Kontrollmaßnahme zu überzeugen. Der Oberste Gerichtshof (OGH) verlangte in seinem Urteil vom 14. Juli 2022⁵, es müsse festgestellt werden, ob ein verwendetes System tatsächlich in der Lage ist, die Menschenwürde zu berühren, um eine Betriebsvereinbarungspflicht daraus abzuleiten.

→ **Ob eine Kontrollmaßnahme die Menschenwürde berührt, hängt ab von:**

- **Häufigkeit der Kontrolle,**
- **Intensität der Kontrolle (inwieweit die Privatsphäre berührt wird) und**
- **Eignung des Kontrollsystems.**

Eine Betriebsvereinbarung (BV) muss auch bei der „*Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers, die über die Ermittlung von allgemeinen Angaben zur Person und fachlichen Voraussetzungen hinausgehen*“ (§ 96a Abs. 1 ArbVG) abgeschlossen werden, sowie bei der „*Einführung von Systemen zur Beurteilung von Arbeitnehmer:innen des Betriebes, sofern mit diesen Daten erhoben werden, die nicht durch die betriebliche Verwendung gerechtfertigt sind*“ (§ 96a Abs. 1 ArbVG). Stimmt der Betriebsrat der Verwendung eines solchen Systems nicht zu, kann die Zustimmung auf Grundlage einer Entscheidung der Schlichtungsstelle ersetzt werden („**ersetzbare Zustimmung**“).

→ **Der Betriebsrat muss das konkrete System und dessen „Hinausgehen über allgemeine Angaben“ oder dessen „Berühren der Menschenwürde“ darstellen, um vor einer Schlichtungsstelle am Arbeits- und Sozialgericht für die Notwendigkeit einer Betriebsvereinbarung zu argumentieren.**

Dabei sind der Rechtsschutz der Gewerkschaften und/oder die betriebsbetreuenden Kolleginnen und Kollegen aus den Gewerkschaften gerne behilflich.

Obwohl das Gesetz von der „**Einführung**“ von Systemen spricht, bezieht sich dieser Absatz auch auf bereits bestehende Systeme. Erweiterung, Abänderung, Verknüpfung zweier Systeme oder die teilweise Rücknahme sind damit gleichfalls gemeint. Werden beim Einsatz von MS 365 also substantielle Updates vorgenommen, so darf dies jeweils nur nach Zustimmung des Betriebsrates geschehen. Ist sowohl nach § 96 als auch nach § 96a ArbVG eine Betriebsvereinbarung abzuschließen, geht die stärkere Vorschrift vor, also § 96 ArbVG. In derartigen Fällen kann die Zustimmung des Betriebsrates nicht durch eine Entscheidung der Schlichtungsstelle ersetzt werden.

Es ist zwar unwahrscheinlich, aber es könnte sein, dass Anwendungen von MS 365 so im Betrieb verwendet werden, dass sie weder eine Kontrollmaßnahme darstellen noch Datenverwendungen beinhalten, die über gesetzliche Vorgaben

Handlungsmöglichkeiten des Betriebsrates

3

hinausgehen und somit weder § 96 noch § 96a ArbVG auf die konkrete betriebliche Verwendung von MS 365 zutreffen. Dann bestehen immer noch weitere Paragraphen, die BV-Tatbestände sind, die also dafür sorgen, dass eine Betriebsvereinbarung abgeschlossen werden muss.

So ist die „*Verwendung von **Betriebsmitteln***“ gemäß § 97 Abs. 1 Ziffer 6 ArbVG mit einer Betriebsvereinbarung zu regeln. Da MS 365 ein „**digitales Werkzeug**“ für die Bearbeitung zahlreicher betrieblicher Aufgaben ist, trifft der Begriff „Betriebsmittel“ auf diese Software zu.

Ebenso kann § 97 Abs. 1 Z 1 ArbVG bei MS 365 tangiert sein, wo geregelt ist, dass „*Allgemeine **Ordnungsvorschriften**, die das Verhalten der Arbeitnehmer im Betrieb regeln*“ in einer BV zu vereinbaren sind. Gäbe es beispielsweise Richtlinien im Betrieb darüber, wie Anwendungen von MS 365 einzusetzen sind (z. B. welche Aktivitäten mit Copilot erlaubt sind und welche nicht oder wie Videocalls auf Teams zu bedienen sind), könnte das unter den Begriff „Ordnungsvorschrift“ fallen.

Sollten sich Arbeitgeber:in und Arbeitnehmer:innenvertretung nicht auf eine Betriebsvereinbarung gemäß § 97 Abs. 1 bis 6 einigen, kann eine Schlichtungsstelle einberufen werden, um die endgültige Entscheidung über die Inhalte einer BV zu treffen.

Es stehen dem Betriebsrat also einige rechtliche Bestimmungen zur Verfügung, mit denen die Interessen der Belegschaft vertreten und durchgesetzt werden können. Je nachdem wofür MS konkret eingesetzt wird, wird ein anderer BV-Tatbestand gelten.

Microsoft und die Arbeitsverfassung

Microsoft 365 und der Datenschutz

3.1

3.2

INSTRUMENTE DES BETRIEBSRATS



Gewerkschaft GPA

© Gewerkschaft GPA

Besteht in einem Unternehmen **kein Betriebsrat**, so schreibt § 10 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG) vor, dass Kontrollmaßnahmen und technische Kontrollsysteme, welche die Menschenwürde berühren, nur dann eingeführt werden dürfen, wenn die oder der betroffene Arbeitnehmer:in zugestimmt hat. Es muss also jede und jeder Beschäftigte, die oder der einer derartigen Kontrolle unterworfen werden soll, zustimmen.

3.2 Microsoft 365 und der Datenschutz

Das Datenschutzrecht spielt eine wesentliche Rolle beim Einsatz von MS 365. Auch Datenverwendungen im Arbeitsverhältnis müssen sich an die „Spielregeln“ der DSGVO halten.

3.2.1 Rechte der betroffenen Arbeitnehmer:innen

Werden personenbezogene Daten verarbeitet, haben die Betroffenen, also diejenigen, um deren Daten es geht, eine Reihe von individuellen Rechten zur Durchsetzung ihres **Grundrechts auf Datenschutz** (§ 1 DSGVO), darunter das Recht auf Auskunft, Berichtigung und Löschung (Art. 15 ff. DSGVO).

Betroffene, also Beschäftigte, die MS 365-Anwendungen nutzen (müssen) und deren personenbezogene Daten verarbeitet werden, haben Anspruch auf **Aus-**

kunft darüber, wer welche (Kategorien) ihrer personenbezogenen Daten zu welchem Zweck und auf welcher Rechtsgrundlage verwendet, für welchen Zeitraum die Daten aufbewahrt bzw. gespeichert werden und – falls es nicht ohnehin eindeutig ersichtlich ist – auf welchem Weg die Daten an die verantwortlichen Personen gelangt sind sowie an welche Empfängerkreise die Daten weitergegeben werden bzw. wurden. Die oder der Verantwortliche hat auf ein solches Auskunftsbegehren binnen vier Wochen Auskunft zu geben.

Gemäß gesetzlicher Definition gehören zu den **personenbezogenen Daten** nicht nur landläufig bekannte Angaben wie Name, Geburtsdatum oder Anschrift, sondern auch IP-Adresse, Standort, Handynummer, Zimmernummer, Personalnummer, Personenkennzeichen wie die Sozialversicherungsnummer oder das Nummernschild eines Autos; kurz: alle Daten, die einer oder einem Beschäftigten eindeutig – egal ob direkt oder indirekt – zugeordnet werden können.

Bewahrt die oder der Verantwortliche unrichtige bzw. nicht aktuelle Daten auf, so hat die betroffene Person das Recht, eine **Berichtigung** der vorhandenen personenbezogenen Daten zu verlangen.

Zudem kann die betroffene Person verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, soweit keine rechtliche Verpflichtung zur Aufbewahrung besteht. Dieses **Recht auf Löschung** gilt, wenn Daten ohne Rechtsgrundlage erhoben wurden oder wenn der Verwendungszweck nicht mehr gegeben ist, sie also nicht mehr gebraucht werden. Grundsätzlich dürfen Verantwortliche die personenbezogenen Daten der Beschäftigten nicht ewig aufbewahren, sondern nur, solange ein Zweck für ihre Verwendung gegeben ist. Liegt der Zweck nicht mehr vor bzw. ist er bereits erfüllt, so sind die personenbezogenen Daten zu löschen – unabhängig davon, ob ein Löschbegehren gestellt wurde oder nicht. Um dieser Pflicht nachzukommen, empfiehlt es sich, automatisierte Löschroutinen zu etablieren.

→ **Stets müssen eine Rechtsgrundlage oder ein (Verarbeitungs-)Zweck vorliegen.**

Zugegeben, bei MS 365 ist es schwierig für die oder den Verantwortlichen, diese Rechte zu erfüllen. Mitunter fehlt es an Wissen, welche Daten verwendet werden, ob sie an Dritte wie MS und dessen Subunternehmen weitergeleitet werden, oder wie lange sie aufbewahrt werden. Arbeitgeber:innen müssen sich freilich dieser Verantwortung stellen. Sie müssen in ihrem Unternehmen die datenschutzrechtlichen Grundlagen so gut wie möglich erfüllen, also Auskunft erteilen, eine Rechtsgrundlage anführen, den Verwendungszweck festlegen.

3.2.2 Übermittlung von Daten (in einen Drittstaat) und der Auftragsdatenverarbeitungsvertrag

Unternehmen müssen personenbezogene Daten nicht zwangsläufig selbst verarbeiten, sondern können auf (Sub-)Unternehmen zurückgreifen, die Datenverarbeitungen in ihrem Auftrag vornehmen. Diese beauftragten Unternehmen werden in der DSGVO als „Auftragsdatenverarbeiter“ bezeichnet. Die Übermittlung von personenbezogenen Daten an Auftragsdatenverarbeiter:innen bedarf einer Rechtsgrundlage – eines sogenannten Auftragsdatenverarbeitungsvertrags (AVV). Dieser dient dazu, die Rechte und Freiheiten der Personen zu schützen und muss Datenart, Verwendungszweck, Speicherdauer, die Pflichten der verantwortlichen Person sowie der Auftragsdatenverarbeiterin bzw. des Auftragsdatenverarbeiters beinhalten.

Microsoft bietet dafür **Standardverträge** an. Im September 2022 wurde der AVV von MS an die durch ein EuGH-Urteil entstandene Rechtslage⁶ angepasst und MS nennt ihn (derzeit) „Microsoft Products and Services Data Protection Addendum (DPA)“⁷. Mittels dieser Verträge soll die Verwendung personenbezogener Daten bei MS in den USA legalisiert werden.

Dass MS Daten von EU-Bürger:innen in den USA verarbeitet, war – und ist – problematisch. Der EuGH hat (bereits mehrmals) festgestellt, dass der Schutz von Daten von EU-Bürger:innen in den USA nicht im selben Ausmaß gegeben ist wie in Europa.⁸ Derzeit gilt das von der EU-Kommission und den USA am 10. Juli geschlossene Abkommen für den rechtmäßigen Datentransfer zwischen USA und EU; die „**Adequacy decision for the EU-US Data Privacy Framework**“(DPF)⁹.

Bei den davor gültigen Abkommen zum Datentransfer zwischen USA und EU, „Safe Harbor“ und „Privacy Shield“, war das „Ablaufdatum“ schnell erreicht. Es bleibt abzuwarten, wie lange die jetzt gültige Vereinbarung hält.

Die meisten Server für europäische MS-Kundinnen und -Kunden stehen mittlerweile in Europa. Dennoch kann Microsoft nicht gänzlich ausschließen, dass personenbezogene Daten in den USA verarbeitet werden und somit nach US-amerikanischem Recht den dortigen Geheimdiensten zur Verfügung gestellt werden. Microsoft versucht zwar, eine solche Auslieferung zu unterbinden, doch das gelingt nicht immer.

3.2.3 Datenschutz-Folgenabschätzung (DSFA)

Die DSFA soll dazu dienen, bereits im Vorfeld einer Datenverarbeitung Risiken für die Betroffenen zu erkennen, Gegenmaßnahmen zu ergreifen und nicht zuletzt durch Datenschutzverletzungen entstehende Nachteile zu minimieren, wozu auch wirtschaftliche Nachteile zählen können (z. B. Kosten, falls Daten aufwendig wiederbeschafft werden müssen, oder eine schlechtere Auftragslage, falls Vertrauensverlust durch einen Datenmissbrauch entstanden ist).

Um festzustellen, ob eine DSFA erstellt werden muss, sollte vorab in einer sogenannten „**Schwellenwertanalyse**“ eingeschätzt werden, welches Risiko für die Grundrechte der Nutzer:innen bei den verwendeten MS 365-Apps besteht. *„Wird bei der Nutzung der Systeme in die Privatsphäre der Beschäftigten eingegriffen?“*, lautet die maßgebliche Frage für die Schwellenwertanalyse.

Ist das Risiko hoch, dass die Privatsphäre der Beschäftigten beeinträchtigt wird, muss die oder der Arbeitgeber:in eine Datenschutzfolgenabschätzung durchführen und darin Abhilfemaßnahmen festlegen. Der Betriebsrat ist bei der Datenschutzfolgenabschätzung einzubeziehen (Art. 35 Abs. 9 DSGVO). Dabei kann sich herausstellen, dass Systemanpassungen bei MS 365 zur Risikominimierung beitragen können. *„Gibt es Einstellungen, die die Privatsphäre besser schützen würden?“*, lautet die maßgebliche Frage, um Abhilfemaßnahmen zu finden.

Bei der DSFA ist der oder die betriebliche Datenschutzbeauftragte beizuziehen. Zusätzlich sind die **Standpunkte der Betroffenen und ihrer Vertretung** anzu-

hören (Art. 35 Abs. 9 DSGVO). Die DSFA ist – neben Artikel 88 DSGVO – die einzige Stelle in der DSGVO, in der explizit Mitwirkungsrechte der betrieblichen Interessenvertretung, also des Betriebsrats, angesprochen sind. Verantwortlich für die Durchführung der DSFA bleibt die bzw. der Arbeitgeber:in – und nicht der Betriebsrat.

Die systematische Auswertung des Nutzer:innenverhaltens und die Verknüpfung großer Mengen von Daten, wie sie bei MS 365 typisch sind, bedingen es, dass eine DSFA durchgeführt werden muss.

→ **Um MS 365 in Betrieben einsetzen zu können, ist eine Betriebsvereinbarung gemäß ArbVG erforderlich. Artikel 88 der DSGVO ermöglicht ebenfalls, dass eine Betriebsvereinbarung abgeschlossen wird „zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten (...), der Organisation der Arbeit (...), der Gesundheit und Sicherheit am Arbeitsplatz ...“.** ¹⁰ **ArbVG und DSGVO ergänzen einander.**

Mit einer Betriebsvereinbarung können jedoch datenschutzrechtliche Mängel nicht beseitigt werden. Selbst wenn sich die BV darauf beruft, gemäß Artikel 88 der DSGVO eine Rechtsgrundlage für die Datenverwendung von MS 365 zu sein, so kann dennoch im Umkehrschluss mittels BV nicht „beschlossen“ werden, dass MS 365 DSGVO-konform sei. Die BV kann allenfalls durch geeignete Maßnahmen die (technischen) Unzulänglichkeiten in Anwendungen von MS 365 korrigieren.

Eine Betriebsvereinbarung ändert nichts daran, dass die grundsätzliche datenschutzrechtliche Verantwortung bei der oder dem Arbeitgeber:in liegt. Das Bestehen einer Betriebsvereinbarung ändert nichts daran, dass die EU-Datenschutz-Grundverordnung (DSGVO) und das österreichische Datenschutzgesetz (DSG) angewendet werden müssen. Eine Betriebsvereinbarung kann die datenschutzrechtlichen Mängel von MS 365 nicht beseitigen, sondern nur versuchen, bestmöglich bei der betrieblichen Verwendung Abhilfe zu schaffen (etwa indem Apps deaktiviert werden).

Immer wieder wird MS dafür kritisiert, sich nicht an die Datenschutzgrundverordnung (DSGVO) zu halten:

Datenschutzfreundliche Voreinstellungen bzw. die Möglichkeit, selbst definierte Einstellungen zum Datenschutz zu treffen, sogenannter „Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen“, wie sie in Artikel 25 DSGVO festgelegt sind, bietet MS 365 nur in begrenztem Maße an. Es besteht nicht immer die Möglichkeit, Privatsphäre selbst zu gestalten („Privacy by default“) bzw. sie abzuschalten (Pseudonymisierung oder „Opt-out“).

MS behauptet, **Auftragsdatenverarbeiter** zu sein und somit seine Dienstleistungen ausschließlich im Auftrag der Kundinnen und Kunden bzw. Unternehmen zur Verfügung zu stellen (gemäß Art. 4 Z 8 DSGVO). MS betreibt aber gleichzeitig Auswertungen im eigenen Interesse.

MS 365 ermöglicht es, **Profile** über einzelne Nutzer:innen zu erstellen. MS 365 erstellt diese Profile auf Basis intransparenter Parameter. Die Erstellung von Profilen erfolgt, ohne dass die Informationspflichten gegenüber den Betroffenen, also den Nutzerinnen und Nutzern, eingehalten werden. Diese Information müsste den Zweck, den Empfängerkreis und die den Profilen zugrunde liegende Logik beinhalten. Zudem besteht die Gefahr, dass Arbeitgeber:innen auf der Grundlage der von MS analysierten Daten Entscheidungen über Beschäftigte treffen könnten (z. B. karrierefördernde Schritte oder auch Karrierehemmnisse). Sollten derartige schwerwiegende Entscheidungen rein auf den automatisierten Profilen von MS beruhen, wäre das Profiling (gemäß Art. 4 Z 5 DSGVO) und unzulässig (Art. 22 Abs. 1 DSGVO).

Es fehlt meistens eine **Datenschutz-Folgenabschätzung** (DSFA) (Seite 26). Zwar besteht ein Angebot von MS, diese DSFA mitzuliefern, doch stellt sich die Frage, ob diese ausreichend an die betrieblichen Gegebenheiten angepasst ist bzw. ob der Hersteller einer Software generell überhaupt dazu berufen ist, deren Einsatz konkret einzuschätzen oder ob man damit nicht sprichwörtlich den „Bock zum Gärtner“ macht.

Es wurden und werden immer wieder **Sicherheitslücken** festgestellt. Im März 2021 wurde z. B. bekannt, dass der Exchange Server mehrerer deutscher Bundes-

behörden gehackt worden war. Im Juni 2024 wurde bekannt, dass MS offensichtlich den Zugangsschlüssel zur Azure Cloud verloren hatte. Im Juli 2024 verursachte ein Security-Update des Auftragsverarbeiters CrowdStrike weltweite Shut-downs (deutsch: Betriebsstilllegung, Stillstand, Abschaltung), unter anderem in der öffentlichen Infrastruktur. Eigentlich müsste es aber geeignete Maßnahmen geben, um Derartiges zu verhindern (Art. 25 DSGVO).

→ **Es stellt sich die Frage, auf Basis welcher Rechtsgrundlage MS 365 von den Verantwortlichen, also den Arbeitgeberinnen und Arbeitgebern, eigentlich verwendet werden kann (siehe Art. 5 DSGVO).**

Die freiwillige Einwilligung ist im Arbeitsverhältnis nicht gegeben. Eine vertragliche oder rechtliche Verpflichtung zur Verwendung von MS 365 wird wohl in den seltensten Fällen vorliegen. Lebenswichtige Interessen sind nur sehr schwer vorstellbar und öffentliche Interessen werden bei Privatunternehmen ebenso wenig vorhanden sein. Es bleiben eigentlich nur noch die **„berechtigten Interessen des Verantwortlichen“** als Rechtsgrundlage, und diese gilt es **zu prüfen, ob nicht „die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern“, überwiegen.**

Um MS 365 zu nutzen, müssen die Betroffenen die Datenschutzerklärungen von Microsoft hinnehmen und in die Verarbeitung ihrer Daten einwilligen. Insbesondere im Arbeitsverhältnis mangelt es solchen Zustimmungserklärungen an der **Freiwilligkeit**. Wegen des Machtgefälles zwischen Arbeitgeber:in und Arbeitnehmer:in kann es **keine echte Freiwilligkeit** geben. Die Freiwilligkeit ist aber ein wesentlicher Bestandteil einer Zustimmung zur Datenverwendung (gemäß Art. 4 Z 11 DSGVO).

MS gibt Daten europäischer Kundinnen und Kunden an US-amerikanische Behörden zur **Strafverfolgung** weiter. Das ist nach US-amerikanischem Recht so bestimmt und wird von Microsoft auch zugegeben.¹¹ MS gibt regelmäßig einen Report heraus, den „Law Enforcement Request Report“, wo anonym aufgelistet

wird, welchen Anfragen seitens der US-Behörden nachgekommen wurde.¹² Hier liefert MS ein Beispiel für seine transparente Informationspolitik.

Zusammenfassung datenschutzrechtlicher Schwierigkeiten

Zusammenfassung datenschutzrechtlicher Schwierigkeiten beim Einsatz von MS 365:

- Es fehlt eine Rechtsgrundlage für die Verwendung von Telemetriedaten seitens MS.
- Die Rechenschaftspflicht kann seitens der Verantwortlichen, also der Unternehmen, nur schwer erfüllt werden, da MS nur begrenzt offenlegt, wie die Daten verarbeitet werden.
- Ein eindeutiger Zweck für die zahlreichen angebotenen Apps ist nicht immer gegeben. Es ist nicht eindeutig feststellbar, wann MS Daten im Auftrag seiner Kundinnen und Kunden verarbeitet und wann es Daten für eigene Zwecke verarbeitet.
- MS löscht personenbezogene Daten nach Erbringung der vereinbarten Leistung nicht immer. Insbesondere Daten zur „Cyberabwehr“ oder im Rahmen von KI-Anwendungen werden nicht vernichtet (bzw. zurückgegeben).
- Datenschutz-Folgenabschätzungen werden bloß standardmäßig, selten jedoch unternehmensspezifisch durchgeführt.
- Personenbezogene Daten aus einer Anwendung werden für diverse Zwecke in anderen Anwendungen weiterverwendet (das Koppelungsverbot wird nicht eingehalten).

3.3 Microsoft 365 und die Künstliche Intelligenz (KI)

Das Wichtigste zuerst: Die EU-Verordnung zur **Künstlichen Intelligenz** hält fest, dass:

„(...) die Verwendung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person in den Bereichen Arbeitsplatz (...) und Bildungsinstitutionen **nicht erlaubt** ist. (Art. 5 (1) f) EU KI-VO).“

Für Arbeit und Bildung (darunter sind Schulen, aber auch Erwachsenenbildungseinrichtungen zu verstehen) gelten also besondere Regeln; die Menschen dort werden besonders geschützt, weil sie sich in einem gewissen Abhängigkeitsverhältnis befinden. Es darf also beispielsweise aus der Aufnahme eines Videos nicht mittels KI herausgelesen werden, ob bei dem Meeting „gute Stimmung“ geherrscht hat.

In der EU-Verordnung zur Künstlichen Intelligenz (KI-VO) ist festgelegt, wie es mit der Verantwortung für KI aussieht. Je nachdem, welche Rolle eingenommen wird (Entwickler:in, Anbieter:in, Betreiber:in, Nutzer:in), abhängig davon, welche Risikostufe die KI hat (niedrig, mittel, hoch, verboten), und je nachdem, wo sie wofür eingesetzt wird (öffentliche Hand, kritische Infrastruktur, allgemein), hält die KI-VO Verpflichtungen fest. Die wichtigsten im Zusammenhang mit dem Arbeitsleben sind:

- **KI-Kompetenz** nachweisen, was in der Regel über Schulungen und Unterweisungen stattfindet und wobei der BR sich an den jeweiligen Ausbildungen beteiligen kann;
- **Menschliche Aufsicht**, wobei der BR überprüfen kann, ob diese gewährleistet ist;
- **Risikomanagement** betreiben, wobei der BR sich die entsprechenden Unterlagen zeigen lassen kann und seine Meinung zu den gesetzten Maßnahmen mitteilen kann;
- Technische **Dokumentation** garantieren, wobei der BR sich die relevanten Informationen erklären lassen kann;
- **Transparenz** und Informationsbereitstellung, wobei der BR sich diese Informationen zunutze machen kann, um eine allfällig erforderliche Betriebsvereinbarung zu verhandeln;
- **Aufzeichnung** von Ereignissen und deren Meldung (Cybersicherheit), wobei der BR sich diese Dokumente zeigen lassen kann und sich an der Entwicklung vorbeugender Maßnahmen – sofern sie die Beschäftigten betreffen – zu beteiligen

Eine direkte Mitbestimmung der (über-)betrieblichen Interessenvertretung ist in der KI-VO nicht verankert. Aus den oben angeführten Pflichten und dem ArbVG lässt sich dennoch ableiten, wo Betriebsrätinnen und Betriebsräte sich beteiligen können und sollen.

MS beschäftigt sich derzeit intensiv mit dem Ausbau von KI. Als Basis für die zahlreichen Varianten der Microsoft-eigenen KI **Copilot** dient dabei „ChatGPT“, das Produkt des Unternehmens „OpenAI“, bei dem Microsoft mit derzeit etwa 27 Prozent größter Einzelinvestor ist – zwar nicht mehr exklusiv, aber ChatGPT läuft vorwiegend in der MS Cloud Azure.¹³

Künstliche Intelligenz ist in zahlreiche Anwendungen von MS 365 eingeflossen, beispielsweise im Rahmen von Textanalyse (Copilot für Word), beim Protokollieren von Meetings (Copilot Teams), beim „Erkennen“ von Gefühlen (Copilot for Service) oder bei einer Kundenanalyse, die die wahrscheinlich auftretende Zufriedenheit prognostiziert (AI Agent) (siehe Seite 70).

3.4 Microsoft 365 und der Gesundheitsschutz

Meist treten gesundheitliche Auswirkungen im Hintergrund auf und ihnen wird wenig Beachtung geschenkt. Schutzmaßnahmen für die Gesundheit der Beschäftigten gelten generell, also nicht nur für (neue) Technologien oder digitale Betriebsmittel wie MS 365. MS 365 kann durch gestiegene Kontrollmöglichkeiten und eine gestiegene **Kontrollhäufigkeit psychische Belastungen** hervorrufen. Es kann **Stress** durch eine Überzahl an Kommunikationskanälen entstehen. Es kann **Unsicherheit** durch mangelndes Wissen entstehen, was wiederum die Fehleranzahl erhöhen kann. Es kann zu einer **Überforderung** kommen, weil eine Schulung unzureichend war oder gleich ganz unterblieben ist und Beschäftigte nicht genau wissen, wie sie die digitalen Werkzeuge von MS 365 bedienen sollen.

→ **Das ASchG bietet im Zusammenhang mit MS 365 Ansatzpunkte für betriebsrätliches Handeln (z. B. Unterweisungspflicht, Evaluierungspflicht).**

Betriebsrätinnen und Betriebsräte können **Schulungen** und Qualifizierungen für die Beschäftigten (gemäß §§ 12–14 ASchG) verlangen oder auf einer Unterweisung beharren, die konkret darstellt, wie die „Betriebsmittel“ verwendet werden sollen, denn im Grunde ist die Software von MS nichts anderes.

Die **Evaluierung** gilt nicht ausschließlich für altbekannte Gesundheitsrisiken (wie Lärm, Kälte oder Schmutz), sondern auch für Gesundheitsbeeinträchtigungen wie Stress oder Furcht (vor Fehlern). Das ASchG gibt vor, wie eine Evaluierung – auch psychischer – Gesundheitsrisiken durchgeführt wird (§ 4 f. ASchG) und wie Informationen zum Gesundheitsschutz verbreitet werden müssen (§ 12 ff. ASchG). Um die Risiken für die Gesundheit der Beschäftigten zu minimieren, muss die oder der Arbeitgeber:in **Maßnahmen** im Sinne des Gesundheitsschutzes ergreifen (gemäß § 4 ASchG). Diese könnten ebenfalls in einer BV festgehalten werden; solche Maßnahmen decken sich mit den in der DSGVO verankerten Vorgaben zu privatsphärefreundlichen Einstellungen (z. B. Deaktivieren der Statusinformation, Begrenzen der Kommunikationskanäle, Recht auf Abschalten etc.).

Die Betriebsrätin oder der Betriebsrat kann und soll **Einsicht** in die Ergebnisse der Evaluierung und der Abhilfemaßnahmen gegen gesundheitliche Gefahren verlangen (siehe §§ 4 und 5 ASchG).

3.5.1 Die Evaluierung

MS 365 ist ein komplexes, sich stets veränderndes System. Es braucht Vorkehrungen, damit die Beschäftigten nicht übermäßig überwacht, permanent analysiert und (fremd-)gesteuert werden. In regelmäßigen Abständen sollte man sich die Mühe machen, das System zu evaluieren. Dabei gilt es zu überprüfen, ob die Bestimmungen der BV eingehalten werden, die Einstellungen noch aktuell sind und/oder neue Apps, neue Features hinzugekommen sind. Ohne eine kontinuierliche Begleitung mittels Evaluierung wird es schwierig, so flexible und vielfältige Systeme wie die von MS 365 unter Kontrolle zu behalten.

Bei einer Evaluierung sollte klargestellt werden:

- wer sie durchführt (Hauptverantwortliche:r und Ansprechpartner:in),

Handlungsmöglichkeiten des Betriebsrates

- wer daran beteiligt ist (evtl. besondere Zielgruppe),
- welcher Zeitraum betrachtet wird,
- welche Methoden eingesetzt werden (z. B. Fragebogen, Interviews, Beobachtungen, Gesundheitszirkel, Unterlagen des Arbeitsinspektorats),
- wo die Abläufe festgehalten werden (z. B. in einer Betriebsvereinbarung) und
- dass **Ergebnisse und Maßnahmen** in den Sicherheits- und Gesundheitsschutzdokumenten zu vermerken sind (§ 5 ASchG).

Um konkrete Maßnahmen zu entwickeln, ist das **S-T-O-P-Verfahren** ausgezeichnet geeignet. Man geht dabei entlang eines abgestuften Prozesses vor, wobei die nächste Stufe erst betreten wird, wenn die vorangegangene erfolglos blieb bzw. wenn auf der vorangegangenen nicht schon alle Zielsetzungen zufriedenstellend erreicht worden sind (sogenannte „**Maßnahmenverdichtung**“).

1. **Substitution:** Bei einer solchen Maßnahme wird eine störende, die Gesundheit beeinträchtigende Gefahrenstelle abgeschafft oder durch eine weniger belastende ersetzt. Das kann durch eine bauliche Maßnahme oder eine andere analoge Vorrichtung geschehen (z. B. werden Rechner mit sensiblen Daten in einen Tresor gestellt oder das Mitlesen auf dem Laptop wird durch eine Folie verhindert). Ein anderes Beispiel wäre, dass Viva Insights deaktiviert wird, weil es aufgrund seiner Datenfülle ohne Zweckbindung und ohne Berechtigungskonzept (u. a. Pünktlichkeitsmessungen bei Teammeetings) bei den Beschäftigten Stress verursacht.
2. **Technik:** Dabei wird ein unerwünschter Zustand durch eine technisch-maschinelle Maßnahme ersetzt. Zwar bietet MS dafür nicht allzu viel Spielraum, die vorhandenen Möglichkeiten sollten aber gesucht und genutzt werden (z. B. Speicherdauer, sogenannte „Retention Policies“ werden reduziert, Einsichtsrechte werden unterbunden, Regelungen zur E-Mail-Weiterleitung eingerichtet, Auswertungen in Power-BI werden pseudonymisiert, ...). Diese Maßnahmen werden in der Regel von der IT-Abteilung umgesetzt.
3. **Organisation:** Sollte eine Verbesserung auf technischer Ebene nicht möglich sein, sind organisatorische Vorgaben das Mittel der Wahl. (z. B. wird die Hand-

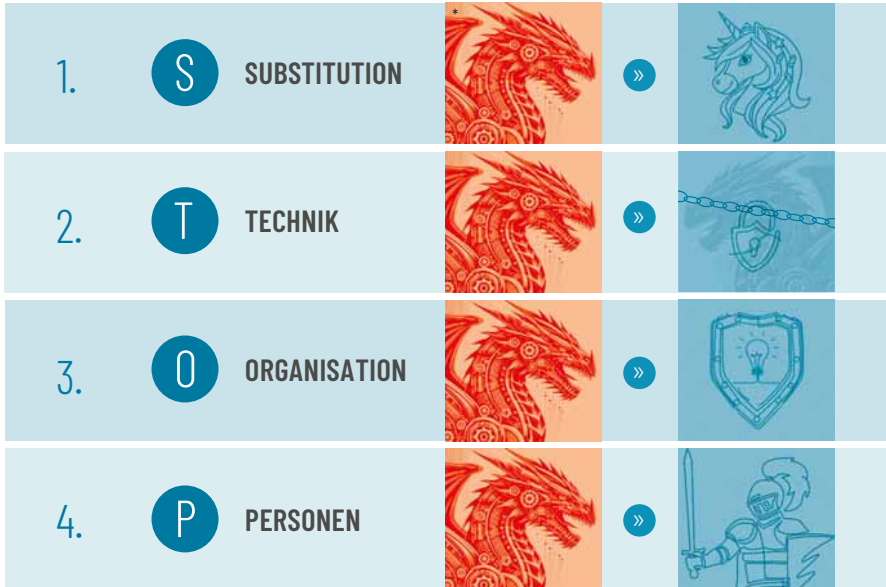
habung von Copilot im gesamten Betrieb deutlich geklärt, geschult und es wird ein:e kompetente Ansprechpartner:in ernannt, damit Unsicherheit und Unklarheiten ausgeräumt werden; Teamleitungen dürfen personenbezogene Verhaltensauswertungen nur unter Hinzuziehung des Betriebsrats ansehen; es wird zwar das Versenden lobender Emojis an Kolleginnen und Kollegen ermöglicht, doch werden diese nicht erfasst und ausgewertet, geschweige denn zu Beurteilungen herangezogen). Hier wird der wichtigste Ansatzpunkt für die Verhandlung der BV liegen.

4. **Person:** Erst wenn alle vorangegangenen, auf der kollektiven Ebene ansetzenden Handlungen nicht den angestrebten Erfolg bringen, ist es angebracht, die Schutzmaßnahmen an einzelnen Arbeitsplätzen in den Fokus zu nehmen oder bei der oder dem einzelnen Arbeitnehmer:in bzw. deren individuellem Verhalten anzusetzen (z. B. Einzelschulung, einzelne Beschäftigte stellen ihre Privacy-Funktionen anders ein, die einzelnen Beschäftigten zu Verhaltensänderungen auffordern).

Handlungsmöglichkeiten des Betriebsrates

DAS S.T.O.P.-PRINZIP

Schutz-Maßnahmen auf Basis des AschG



* Der Drache wurde mit Hilfe von Dall-E erstellt

© Gewerkschaft GPA

Die regelmäßige Evaluierung von MS 365 könnte auch zu den Aufgaben einer **internen MS 365-Gruppe** (Seite 50) zählen. Da MS 365 beständig erweitert und abgeändert wird, sollte am besten kontinuierlich evaluiert werden. Vom Gedanken einer einmaligen Evaluierung oder einer für die Ewigkeit abgeschlossenen BV muss man sich bei MS 365 verabschieden. Eine gute Evaluierung ist ein kontinuierlicher Prozess, der nicht immer leichtfällt, aber es lohnt sich gerade im Hinblick auf MS 365, da dabei auf die vielen Veränderungen und potenziellen Beeinträchtigungen flexibel eingegangen werden kann.¹⁴

→ **Workflows und andere Prozesse, die in MS 365 gesteuert und abgebildet werden, müssen immer auch den „Faktor Mensch“ berücksichtigen und gesundheitsschädliche Auswirkungen abschwächen (vgl. § 7 ASchG). Es**

sind daher regelmäßig unter Hinzuziehung des Betriebsrates Gefährdungsbeurteilungen vorzunehmen und Maßnahmen zu erstellen, um die Gesundheit der Beschäftigten zu schützen (vgl. § 4 ASchG; § 92a Abs. 1 Z 3 ArbVG).

3.5.2 Die Unterweisung

Wenn in einem Betrieb MS 365 eingeführt wird, kommt das meist einer „Einführung oder Veränderung von Arbeitsverfahren“ und der „Einführung oder Verwendung von Arbeitsmitteln“ gleich (§ 14 Abs. 1 ASchG). Es wird beispielsweise mit anderen Mitteln kommuniziert (z. B. Teams Channel, Phone, Outlook etc.), es werden andere Tools für die Erstellung von Dienstplänen verwendet (z. B. Planner, Project, Forms, Dynamics) u. s. w.

Für diese Arbeitsmittel von MS 365 ist eine **Unterweisung gemäß ASchG erforderlich**, zu der auch fachkundige Personen in Sachen **psychischer Belastungen** hinzugezogen werden können. Das empfiehlt sich geradezu angesichts der vielfältigen Kooperations- und Kommunikationsmethoden sowie Überwachungs- und Sicherheitsfeatures, die MS 365 im Angebot hat. Schnell kann dadurch, dass sich die Beschäftigten permanent überwacht fühlen, eine Belastung auftreten. Schnell kann Stress entstehen, wenn unklar ist, mit welchen Personen zu welchen Themen auf welchen Kanälen zu kommunizieren ist. Rasch wird sich jemand überfordert fühlen, wenn auf sämtlichen Kommunikationskanälen Benachrichtigungen eintrudeln, deren Prioritäten nicht klar definiert sind. Wie dem entgegengewirkt werden kann, wäre in einer solchen Unterweisung zu thematisieren.

Die Basis-Betriebsvereinbarung

4

Bei dem Versuch, die Verwendung von MS 365 generell zu unterbinden, handelt es sich aller Wahrscheinlichkeit nach um ein aussichtsloses Unterfangen. MS hat bereits ein viel zu großes Gewicht, als dass ein Unternehmen in Bausch und Bogen darauf verzichten könnte. Der BR kann sich allerdings überlegen, ob er einzelne MS 365-Anwendungen im Betrieb unterbinden möchte. Das wäre möglich, indem er den Abschluss einer BV dazu verweigert; etwa, wenn der begründete Verdacht besteht, dass mit der App überschießende Überwachung der Arbeitnehmer:innen möglich ist.

→ **Ohne Zustimmung des Betriebsrats ist in der Regel der Einsatz der jeweiligen Anwendung arbeitsrechtskonform nicht möglich.**

Der betriebsrätliche Einfluss besteht in der Praxis seltener in einem Verbot, sondern darin, eine Betriebsvereinbarung (BV) abzuschließen. In der BV soll geregelt werden, wie Überwachungsmaßnahmen am Arbeitsplatz vermieden, das minutiöse – wenn nicht sogar „sekundöse“ – Durchleuchten der Arbeitsweise von Beschäftigten unterbunden und so die Privatsphäre und die Menschenwürde der Beschäftigten besser geschützt werden – etwa, indem die Einsicht von Vorgesetzten in bestimmte Datenanalysen unterbunden wird.

MS 365 erfordert den Abschluss einer Betriebsvereinbarung. Sowohl einzelne Anwendungen, die personenbezogene Daten der Beschäftigten verarbeiten, als auch die vielen Kombinations- und Auswertungsmöglichkeiten machen eine (oder mehrere) an die jeweiligen betrieblichen Gegebenheiten angepasste Betriebsvereinbarung(en) erforderlich. MS 365 ist ein Gesamtpaket, das in unterschiedlichster Art und Weise zum Einsatz kommt. Bei der Anwendung von MS 365-Produkten bestehen vielfältige Kombinations- und Anwendungsmöglichkeiten, die sich derzeit ins (fast) Unendliche ausdehnen, da (fast) sämtliche Anwendungen (derzeit) mit KI erweitert werden.

Wie die fertige BV schlussendlich aussieht, hängt davon ab, welches MS-Abonnement ein Unternehmen gebucht hat, beziehungsweise welche Lizenz(en) ein Unternehmen gekauft hat, welche Teile von MS 365 dazugebucht oder (de-)aktiviert wurden, ob es bereits BVen zu ähnlichen Tools und Themen gibt (z. B. eine

Datenschutz-Rahmen-BV) und nicht zuletzt von der Betriebskultur. Was genau in der Betriebsvereinbarung enthalten ist, welche Regelungen im Betrieb hilfreich sind, welcher Umgang passend ist, das wird je nach Branche und Betriebsgröße (und damit verbundenen Ressourcen) unterschiedlich sein.

→ Eine einzige Betriebsvereinbarung kann diesen unzähligen Möglichkeiten wohl kaum gerecht werden. Dieser Abschnitt des Skriptums dient zur Unterstützung, als Ideengeberin, als Textbausteinkasten, um eine maßgeschneiderte Vereinbarung im Betrieb argumentieren und abschließen zu können.

Im Dreischritt zur Betriebsvereinbarung

- **Schritt eins:** Verschaffe dir einen **Überblick** über (de-)aktivierte Anwendungen im Betrieb. Nutze deine Informations- und Beratungsrechte. **Welche MS 365 Anwendungen werden verwendet?** lautet die Frage, die der BR stellen muss.
 - **Schritt zwei:** Stelle fest, zu welchem **Zweck** eine Anwendung verwendet werden soll. **Wozu sollen die MS 365 Anwendungen verwendet werden?** lautet die Frage, die der BR stellen muss.
 - Auf dieser Basis folgt erst **Schritt drei:** erstelle eine **Betriebsvereinbarung**. **Wie soll MS 365 im Betrieb verwendet werden?** lautet die Frage, die der BR stellen muss.
- Für Unternehmen mit der Lizenz E3 oder E5 („E“ steht für Enterprise, also Unternehmen) stellt Aaron Dinnage, Director of Strategic Customer AI Partnerships bei Microsoft in Australien, regelmäßig eine äußerst hilfreiche Übersicht zusammen: <https://m365maps.com/files/Microsoft-365-Enterprise-All.htm>
- Zusätzlich zu den Gesamtpaketen können Kundinnen und Kunden Erweiterungen erwerben, die sogenannten „related services“. Darunter befindet sich eine eigene Rubrik mit Auswertungen und Darstellungen des

Die Basis-Betriebsvereinbarung

Nutzer:innenverhaltens, die „Employee Experience“: Diese eignet sich besonders zur Überwachung von Beschäftigten und sollte daher vom Betriebsrat genau unter die Lupe genommen werden. <https://m365maps.com/files/Related-Services.htm>

Auf dem Weg zur BV hilft es zu wissen:

- Wer sind die **Ansprechpartner:innen** für den Betriebsrat? Gibt es eine Person oder eine Gruppe, die fix für die BV-Verhandlungen zur Verfügung steht?
- Wann setzt man sich zusammen? Gibt es einen **Zeitplan**, Fristen, bis wann Vorschläge durchgesehen werden und darüber entschieden wird?
- Wie sieht das bestehende **Umfeld** aus? Gibt es bereits BVen zum Thema? Fangen wir bei Punkt null an? Müssen bestehende BVen adaptiert werden?
- Welche **Struktur** soll die BV bekommen? Soll sie ein grober Rahmen sein? Wird es eine Regelung für eine gemeinsame Funktion (z. B. Kommunikation, Security)? Soll eine Anwendung (z. B. Teams) geregelt werden? Soll eine einzelne Funktion (z. B. Standorterfassung) geregelt werden?
- Was sind die wesentlichsten **Punkte**, die vereinbart werden müssen? Gibt es besondere „Knackpunkte“? Bestehen branchenspezifische oder unternehmensspezifische Vorgaben, die es zu berücksichtigen gilt? Haben die Beschäftigten besondere Anliegen?

Worauf soll nun das Augenmerk gelegt werden, wenn eine **allgemeine Basis-Betriebsvereinbarung** zu MS 365 ausverhandelt wird?

4.1 Der Verwendungszweck oder die Zweckbindung

Der Zweck muss eindeutig sein. Das ist eine Grundregel aus der Datenschutz-Grundverordnung (Art. 5 DSGVO). Es muss klar ersichtlich sein, welche Daten wofür verwendet werden.

MS 365 erschwert diese eindeutige Zweckbindung durch seine Architektur, in der alles mit allem verknüpft ist. So kann ein und derselbe Zweck mit unterschiedlichen MS Anwendungen erfüllt werden (z. B. Projektplanung mit Planner und/

oder Project), bzw. ein und dieselbe Anwendung unterschiedlichen Zwecken dienen (z. B. Teams zur Kommunikation mit Kundinnen und Kunden, die rechtssicher gespeichert werden muss, oder/und zum Plausch mit Kolleginnen und Kollegen, der der Privatsphäre zuzuordnen ist). Es ist je nach Betrieb unterschiedlich, auf welche Art, zu welchem Zweck, in welchem Ausmaß Anwendungen von MS 365 verwendet werden.

Die Verarbeitung personenbezogener Daten im Rahmen der Nutzung der Komponenten von Microsoft 365 lässt sich technisch nicht vermeiden. Aus Gründen der Datenminimierung ist der Zweck der Datenverarbeitung auf das notwendige Maß einzuschränken, und im Folgenden werden die Zwecke, zu denen Beschäftigten mit MS 365 verarbeitet werden dürfen, festgelegt:

- zur Bereitstellung und Nutzung von MS 365 die technisch erforderlichen Nutzer:innendaten;
- zur Unterstützung der Kommunikation und Zusammenarbeit in den einzelnen Teams der Arbeitgeberin bzw. des Arbeitgebers;
- zur Umsetzung und Kontrolle von Datenschutz und IT-Sicherheit;
- zur Dokumentation der zuständigen Bearbeiterin oder des zuständigen Bearbeiters einer Aktivität;
- zur Ermöglichung von Rückfragen, Klärung von Verantwortlichkeiten und Behebung von Fehlern im Einzelfall.



Die Rahmenbetriebsvereinbarung wird geschlossen, um eine erfolgreiche Umsetzung der Einführung und Anwendung der E3-Lizenz zu unterstützen, die Beteiligung des Betriebsrates im Rahmen der gesetzlichen Mitbestimmungsrechte zu gewährleisten, den Bedürfnissen der Arbeitnehmer:innen beim Einsatz neuer Anwendungen Rechnung zu tragen und deren Rechte und Pflichten zu regeln.

Ziel dieser Rahmenbetriebsvereinbarung ist es insbesondere mittels Anlagen die zweckgebundene Verarbeitung personenbezogener Daten der Arbeitnehmer:innen in den zum Einsatz gelangenden Komponenten der E3-Lizenz festzuhalten, für die Arbeitnehmer:innen klare Regeln für

die Anwendung der zum Einsatz gelangenden Komponenten der E3-Lizenz zu schaffen und eine unzulässige Weitergabe personenbezogener Daten zu unterbinden.

4.2 Das Berechtigungskonzept oder die Zugriffsbeschränkung

Als Grundregel gilt, dass Daten nur jenen, die sie für ihre Arbeitsaufgaben benötigen zur Verfügung stehen sollen (auch bekannt unter dem „Need-to-Know-Prinzip“). Dies ergibt sich aus dem DSGVO-Grundprinzip der Vertraulichkeit sowie der Datenminimierung.

→ **Berechtigungskonzepte sind restriktiv zu fassen, damit die ohnehin eng verflochtenen Datenkombinations- und Auswertungsmöglichkeiten keine übermäßigen Einblicke in das Verhalten und die „Leistung“ der Beschäftigten ermöglichen. Im Standard-Berechtigungskonzept von MS 365 sind etwa 100 Rollen vorgesehen, womit die Einsichtsrechte zweckmäßig gestaltet werden können.**

Der **Betriebsrat selbst braucht eine Rolle**, damit er überprüfen kann, ob das Rollenkonzept stimmig ist und ob die Vereinbarungen eingehalten werden. Um den Betriebsrat nicht seiner Mitspracherechte zu berauben, ihn aber auch nicht mit unnötigen Informationen zu überfrachten, eignet sich folgende Formulierung aus einer Betriebsvereinbarung.



Der Betriebsrat hat jederzeit zur Ausübung seiner Rechte ein separates Konto mit globalen Leserechten in dem Produktiv-Mandanten von MS 365. Zusätzlich erhält der Betriebsrat Zugriff auf ein Auditierungswerkzeug mit Leserechten für das Nachvollziehen der Konfigurationseinstellungen sowie der Aktivitäten der Administrations-User in dem MS 365 Produktiv-Mandanten.

4.3 Die Speicherdauer

Manche Auswertungen in MS 365 bauen auf langfristigen Datenhistorien auf. Die gesetzliche Grundregel für Löschfristen, wonach personenbezogene Daten nur so lange aufbewahrt werden dürfen, wie sie ihren Zweck erfüllen, wird dadurch konterkariert. Innerbetrieblich muss ein Vorgehen vereinbart werden, wie man nicht mehr benötigte Daten „außer Betrieb nehmen“ kann bzw. diese nicht mehr eingesehen, ausgewertet, verglichen etc. werden können. Auch wenn die technische Möglichkeit zu langfristigen Datenspeicherungen besteht, sollte in der BV festgelegt werden, dass es unzulässig ist, sämtliche technischen Möglichkeiten auch praktisch zu nutzen. „Technisch möglich – organisatorisch untersagt“ sollte der Wahlspruch lauten. Das ist schon allein deshalb wichtig, damit man das Prinzip der „Datenminimierung“ (gemäß Art. 5 Abs. 1c DSGVO) einhält und damit „technische und organisatorische Maßnahmen“ (gemäß Art. 32 DSGVO) getroffen werden.

4.4 Die Privatnutzung

MS 365 ist (fast) immer auch ein Werkzeug für Kommunikation und Zusammenarbeit und ist (nahezu) jederzeit und von überall erreichbar, wodurch extensives Arbeiten und damit eine Ausdehnung von Arbeitszeit und Erreichbarkeit geradezu herausgefordert werden. E-Mails werden vor dem eigentlichen Arbeitsbeginn gelesen, Dokumente nach Arbeitsende bearbeitet ... MS 365 bietet einen ganzen „Bauchladen“ an Kommunikations- und Kollaborationstools (z. B. Outlook, Teams, Phone, Chat, Loop, OneDrive, Viva Engage etc.). Das kann – insbesondere, wenn die verschiedenen Möglichkeiten nicht zweckmäßig voneinander getrennt, erprobt und eingeübt sind – zu Verwirrung und Überforderung führen.

MS 365 ermöglicht eine Nutzung, die weit über das Berufliche hinausgeht. Daher sollte die oder der Arbeitgeber:in klar kommunizieren, was in der Arbeitszeit verboten ist (z. B. Spielen, Shoppen) und was geboten ist (z. B. Kundinnen- bzw. Kundengespräche nur mit Teams-Call). Eine Abgrenzung von beruflicher und privater Nutzung, eine Einschränkung der Kommunikationskanäle sowie das **„Recht auf Abschalten“** sind angebracht. Für die Privatnutzung sollte festgelegt sein, wo

gespeichert wird (z. B. verlangen manche Firmen, dass Betriebliches nur im dafür vorgesehenen SharePoint, Privates nur auf OneDrive abgelegt werden darf).



Die Nutzung von MS 365 erfolgt grundsätzlich nur während der Arbeitszeit und ist Arbeitszeit. Arbeitnehmer:innen sind nicht dazu verpflichtet, außerhalb der Arbeitszeit Mitteilungen (oder Anrufe/Calls) zu erhalten, zu lesen oder zu bearbeiten.

4.5 Das Profil

Über – fast den gesamten Tagesverlauf aktive – MS 365 Anwendungen werden Metadaten erstellt und können zu Leistungs- oder Verhaltensprofilen zusammengestellt werden. Es wird über die Verbindungsdaten mitverfolgt, wer wann wo in welche Anwendungen wie lange mit welcher Berechtigung eingeloggt ist. Zu Zwecken der IT-Sicherheit ist das sinnvoll, Vorgesetzte sollten darauf keinen Zugriff haben. Mitunter grafisch aufbereitete Anzeigen des Arbeitsortes, des Arbeitsfortschritts, der Arbeitsleistung, der Kooperationspartner:innen etc. dürfen nicht dazu herangezogen werden, Arbeitsleistung und -verhalten zu kontrollieren oder bestimmte Beschäftigte(-ngruppen) zu diskriminieren. Ein Generalverbot der Leistungs- und Verhaltenskontrolle für Vorgesetzte oder „neugierige“ Kolleginnen und Kollegen sollte in der BV enthalten sein.



Diese Betriebsvereinbarung dient dem Schutz der Mitarbeiter:innen vor überschießenden Kontrollmaßnahmen. Auf die Analyse von Leistungs- und Verhaltensprofilen wird seitens der Vorgesetzten verzichtet (Ausnahmen siehe Anhang). Automationsunterstützte Prognosen zu Leistung und Verhalten sind untersagt.

Nutzer:innen können eigene Profile anlegen, die in verschiedenen Anwendungen angezeigt werden (z. B. Teams, Outlook). Die Freigabe persönlicher Informationen (z. B. Foto, Status, Kontakte ...) sollte freiwillig sein. Die Verweigerung der Freigabe darf keine negativen Konsequenzen für Beschäftigte haben. Es empfiehlt sich, ein Benachteiligungsverbot zu vereinbaren.

4.6 Das (angebliche) Fehlverhalten oder die Kontrolle

Sollten Auswertungen das (angebliche) Fehlverhalten von Beschäftigten beinhalten, so ist ein Vorgehen zu vereinbaren, damit der Sachverhalt, also das (vermutete) Fehlverhalten, geklärt sowie „Beifang“ vermieden und überschießende Folgen verhindert werden.



Wird bei der zulässigen und im Allgemeinen üblichen Verwendung von MS 365 ein Fehlverhalten einer Person festgestellt, wird seitens der IT-Administration gemeinsam mit dem oder der Betroffenen die Ursache hierfür geklärt. Ein Mitglied des Betriebsrates kann dabei hinzugezogen werden.

Erst wenn es sich eindeutig um einen nicht lösbaren, im Bereich des oder der Betroffenen liegenden und auch um keinen technisch bedingten Fehler handelt, werden die oder der Vorgesetzte und ein Mitglied des Betriebsrates informiert und ein ehestmöglicher Gesprächstermin vereinbart.

Auf Wunsch der oder des Betroffenen kann der Betriebsrat zu dem darauffolgenden Gespräch hinzugezogen werden. Ziel des Gesprächs ist es, zukünftiges Fehlverhalten zu vermeiden (z. B. Löschregelungen modifizieren, Schulungen anbieten). Diese vereinbarten Maßnahmen werden schriftlich festgehalten.

Sollte dadurch der Fehler nicht behoben werden und tritt er innerhalb eines halben Jahres erneut auf, ist das beschriebene Prozedere zu wiederholen.

Erst im Anschluss daran dürfen disziplinarische Maßnahmen (z. B. Verwarnung) unter Einbeziehung des Betriebsrates gemäß § 102 ArbVG getroffen werden.

Ausnahmen von dem Vorgehen sind nur dann erlaubt, wenn eine unmittelbare Gefahr für die betriebliche Infrastruktur (z. B. Virenbefall), ein erheblicher wirtschaftlicher Schaden [z. B. Verlust eines Großkunden] oder strafrechtlich relevantes Fehlverhalten (z. B. Geheimnisverrat) vorliegt. In derartigen Notfällen wird die Ausgangslage konkret begründet

und das Konfliktlösungsgespräch darf unterbleiben bzw. erfolgt erst, wenn die Sicherheit des Betriebs wieder gewährleistet ist. Die oder der Arbeitgeber:in verpflichtet sich (und alle allfällig beteiligten Stellen wie den betrieblichen Datenschutzbeauftragten oder die betriebliche Datenschutzbeauftragte, die HR-Abteilung), nur solche Schritte durchzuführen, die für die unmittelbare Abwendung des Schadens bzw. der Gefahr erforderlich sind. Sollten dabei Erkenntnisse über das Verhalten von Beschäftigten gewonnen werden, die nicht mit dem Anlass der Maßnahme in Zusammenhang stehen, dürfen diese nicht verwendet werden. Unabhängig davon, ob der Betriebsrat an Konfliktlösungsgesprächen beteiligt war, wird er einmal im Quartal darüber informiert, wie viele derartige Gespräche stattgefunden haben.

Maßnahmen, die nicht auf Basis der hier vorgegebenen Schritte erfolgen, sind unwirksam und müssen zurückgenommen werden.

Ein anderer Betrieb hält sich kurz und schränkt das Einsichtsrecht für Vorgesetzte ein.



Zur Klärung schwerer arbeitsrechtlicher Pflichtverletzungen, die gleichzeitig eine Straftat darstellen, darf bei begründetem, auf Tatsachen beruhendem, dokumentiertem Verdacht die bzw. der Arbeitgeber:in unter Wahrung des Verhältnismäßigkeitsgrundsatzes und vorheriger Information des Betriebsrates Kontrollmaßnahmen initiieren. (...) Dem Betriebsrat wird ein vollständiges Protokoll der eingesehenen Nutzerdaten zur Verfügung gestellt.

4.7 Die Schulung

Zu jeder aktiven Frontend-Anwendung, also jenen, in denen die Beschäftigten direkt arbeiten, ist eine Schulung anzubieten. Vor allem in der ersten Einführungsphase sind Trainer:innen, Lernbegleiter:innen, Buddies, Mentorinnen bzw. Mentoren sowie Expertinnen und Experten für die Beschäftigten von großem Nutzen. Bei den Schulungen ist es einerseits sinnvoll, die direkte Anwendung und die vielfältigen Möglichkeiten zu erlernen, andererseits sollten auch datenschutzrele-

vante Inhalte in die Schulungen mit einfließen (z. B. wie man Status-Anzeigen unterbindet, wie in den persönlichen Einstellungen „Erfahrungen“ deaktiviert werden können oder wie Daten klassifiziert und damit besonders geschützt werden).



Es werden Schulungen zur Verwendung der Microsoft 365-Dienste angeboten. Schulungen finden grundsätzlich in der Arbeitszeit statt und berücksichtigen die Belange von Teilzeitbeschäftigten. Die gesamte Schulungszeit gilt als Arbeitszeit. Die Schulung erfolgt ungestört und abseits des Normalbetriebs. Die Schulung erfolgt auf Deutsch. Die Schulungen können in Form von Präsenzs Schulungen, Webinaren oder als Selbststudium stattfinden. Die Schulungskosten trägt die bzw. der Arbeitgeber:in. Die Schulung beinhaltet neben den im Betrieb eingesetzten Anwendungen von MS 365 auch Hintergrundinformationen zu datenschutzrelevanten Einstellungen. Lernziele, Zeitplan und Zielgruppen werden den Teilnehmenden bekannt gegeben.

Besonders geschult werden die Informationseigentümer sowie die „Champions“, die die Gruppen in Microsoft 365 Anwendungen administrieren.

In einem Betrieb wird bei den Schulungen explizit auf **Barrierefreiheit** eingegangen:



Der Auftragsverarbeiter hat in seinen Lösungskomponenten Anforderungen der Web Content Accessibility Guidelines (WCAG) 2.0 bzw. 2.1 umgesetzt. Eine umfassende Übersicht zur Barrierefreiheit stellt der Auftragsverarbeiter in seiner Nutzer-Dokumentation unter dem Suchwort „Accessibility“ zur Verfügung.

Für den Fall, dass Mitarbeitende mit körperlichen Einschränkungen weitergehende Unterstützung bei der Nutzung der technischen Einrichtung benötigen, werden die Betriebsparteien gemeinsam mit der lokalen Landesstelle des Sozialministeriumservice eine passende Lösung für die oder den Mitarbeitenden veranlassen.

4.8 Die Updates oder die Aktualisierung

Es erfordert Zeit, den Umgang mit MS 365 Anwendungen zu erlernen. Es sollte daher nicht alles auf einmal freigeschaltet werden und bisher genutzte Systeme nicht von einem Tag auf den anderen abgeschaltet werden. Werden neue Anwendungen der MS-Welt hinzugefügt, ist es sinnvoll, eine **Testphase** laufen zu lassen. Während dieser Testphase kann der BR feststellen, welche Punkte besonders heikel sind und daher in einer BV geregelt werden müssen.

Microsoft spricht von einer „Toleranzphase“ bzw. bei Copilot von einem „Copilot-Lab“. Klar sein muss dabei, dass eine solche „Toleranzphase“ ein Ablaufdatum hat.

Einige Firmen haben vereinbart, Updates vorab nur für eine **Testgruppe** in einem geschützten Bereich verfügbar zu machen („Sandkastenanalyse“) und erst in einem zweiten Schritt für alle Nutzer:innen bereitzustellen. Gibt es derartige Testgruppen, sollte sich der Betriebsrat hineinreklamieren.



Zur besseren Abstimmung (...) zur Versachlichung und Beschleunigung der Mitbestimmungsprozesse und zur regelmäßigen Aktualisierung von Betriebsvereinbarungen (...) sollen regelmäßig einzelne Betriebsratsmitglieder als Test-User in Projekte der IT-Organisation einbezogen werden (...) und ggf. nach Abschluss der Projekte in der Nachbetreuung als Key-User definiert (...) werden. Der Betriebsrat hat das grundlegende Recht, an den Projekten (...) teilzunehmen. Eine Verpflichtung (...) leitet sich daraus jedoch nicht ab. (...) Die Teilnahme als Test-User ist Betriebsratsarbeit und entsprechend in dem erforderlichen Umfang freizustellen. (...) Die Aufgaben der Test-User umfassen insbesondere: das freie Ausprobieren und Prüfen von Funktionalitäten der jeweiligen Services, (...) den Abgleich mit den Projektzielen, (...) die Entwicklung von ergänzenden Vorschlägen und Kriterien für Design- und Customizingphasen, die Teilnahme an Schulungen, (...) die Beteiligung an der Durchführung der Systemtests (...) die Teilnahme an der Evaluation der Test- und Pilotphasen, (...) Zugang zu allen relevanten Unterlagen und Dokumentationen.

Die Updates oder die Aktualisierung 4.8

In einer solchen Testgruppe sollten folgende Fragen besprochen werden:

- Tangiert das **Update** Beschäftigtendaten, deren Auswertung, die Möglichkeiten zur Leistungs- und Verhaltenskontrolle?
- Ändert sich durch die Updates die Arbeitsorganisation, die Zusammenarbeit, die – psychische – **Belastung** der Beschäftigten (z. B. durch permanente Anzeige des Präsenzstatus, automatische Übernahme von Terminen)?
- Hat das Update Auswirkungen auf die **Qualifizierung** der Beschäftigten (z. B. Trainingserfordernisse)?
- Sind die **Privatsphäre-Einstellungen** und **Berechtigungen** nach dem letzten Update noch so, wie sie zuvor waren?

MS 365 beliefert seine Kundinnen und Kunden permanent mit Updates. Für jede IT-Abteilung zählt es zu den großen Herausforderungen, dabei den Überblick zu bewahren. Ein Betriebsrat beschreibt seinen Eindruck so: „Wenn man glaubt, man hat endlich verstanden, wie es funktioniert, dann gibt es ein Update. Und dann ändern sich die Funktionalitäten und man findet nix mehr und muss mit den ganzen Einstellungen wieder von vorne anfangen. Da kannst du nix dran ändern. Das ist, wie wenn im Supermarkt die Regale umgeräumt werden.“



Bei der Einführung, Änderung, Umstellung, Anpassung oder Erweiterung bestehender oder neuer IT-Systeme prüft die IT-Arbeitsgruppe, ob eine Anpassung der Betriebsvereinbarung erforderlich ist und leitet bei Bedarf die notwendigen Schritte ein.

- Es lohnt sich, regelmäßig nachzusehen, welche Veränderungen und welche neuen Möglichkeiten von MS 365 veröffentlicht werden. Die Freigaben (Englisch: Releases) stellt MS 365 auf einer eigenen Webseite übersichtlich gegliedert nach Lizenz, Anwendung und Veröffentlichungsstatus dar (in Entwicklung/in development, gestartet/launched und ausgerollt bzw. seit wann eine Änderung ausgerollt ist): <https://www.microsoft.com/en-us/microsoft-365/roadmap>

Wer sich den allgemeinen Überblick nicht durchlesen möchte, überspringt ihn und klickt auf „jump to roadmap“: [Microsoft 365 Roadmap](#) | [Microsoft 365](#)

4.9 Die Ansprechpartner:innen

Meist werden sie „Power-User:innen“ oder „Key-User:innen“ genannt. Meist sind sie aus dem Kreis der Kolleginnen und Kollegen, also der „normalen“ Nutzer:innen, und werden speziell zu den Anwendungen von MS 365 geschult. Sie bringen IT-Interesse sowie Vorwissen und Neugier mit. Geduld und didaktisches Geschick sind von Vorteil, da sie ihre Kenntnisse weitergeben sollen. Der Nachteil an dem Konzept ist, dass diese Personen eine Verantwortung übertragen bekommen, die schwierig zu erfüllen ist. „Wir sind nichts anderes als billige Hilfskräfte für die Geschäftsführung, damit die sich umfassende professionelle Schulungen für alle ersparen,“ sagt eine Seminarteilnehmerin, die diese Funktion innehat.

Dennoch sind diese kompetenten Ansprechpersonen dringend und notwendig. MS 365 ist ein flexibles und schnelllebiges Programm, das einer eben solchen Auskunftsstelle bedarf. Bei einer umfassenden Software wie MS 365 wird man mit *einer* Person vielleicht nicht das Auslangen finden. Eine eigene, mit möglichst fixen Mitgliedern zusammengesetzte **interne Microsoft-365-Gruppe**, die aus Beschäftigten unterschiedlicher Bereiche sowie Fachexpertinnen und -experten besteht (z. B. IT, HR, Recht, Betriebsrat, Vertrieb, Produktion, Geschäftsführung, betriebliche:r Datenschutzbeauftragte:r, Sachverständige), sich möglichst regelmäßig trifft und sich der Fragen im Zusammenhang mit MS 365 annimmt, ist eine hilfreiche Sache. Eine solche bedarfsorientierte Stelle, die rasch und unkompliziert agieren kann und dafür von anderen Arbeitsaufgaben befreit ist, sollte in einer BV ebenso definiert werden wie Zusammensetzung, Aufgaben, Frequenz der Treffen und Entscheidungsbefugnisse.

Manche Betriebe nennen das „IT-Arbeitsgruppe“, „gemeinsamer MS 365-Ausschuss“ oder „Microsoft-Kommission“.



Zur Evaluierung der Bestimmungen der Vereinbarung, zur Analyse der organisatorischen und technischen Veränderungen sowie als Anlaufstel-

Je für betriebliche Erfahrungen im Umgang mit Microsoft 365 wird eine prozessbegleitende IT-Arbeitsgruppe gebildet.

Treffen finden zumindest einmal pro Quartal statt. (...)

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

Die IT-Arbeitsgruppe setzt sich zusammen aus:

- Leitung IT (Vorschlag: Leitung IT-Arbeitsgruppe),
- IT-Administrator:in (1 st Level Support),
- Abteilung Recht,
- Betriebsrat,
- Datenschutzbeauftragte:r,
- Geschäftsführung,
- im Bedarfsfall externe Beratung.

Um den Umgang mit MS 365 zu schulen und zu üben, holen sich Unternehmen mitunter eigene spezialisierte **externe Berater:innen** an Bord. Der Betriebsrat sollte sich in der BV zusichern lassen, dass auch auf seiner Seite externes Fachwissen hinzugezogen wird. Das kann die Gewerkschaft, die Arbeiterkammer oder ein externer Anbieter sein, der auf die Vertretung der Interessen der Arbeitnehmer:innen und den Privatsphäreschutz spezialisiert ist.



Zur qualifizierten Beurteilung kann der Betriebsrat erforderlichenfalls externe, zur Verschwiegenheit verpflichtete Sachverständige seiner Wahl hinzuziehen. Die bzw. der Arbeitgeber:in erteilt hierzu – nach vorheriger Information – die nach ArbVG erforderliche Zustimmung, um die marktübliche Vergütung sicherzustellen.

Der Überblick und die einzelnen Anwendungen

Um Betriebsvereinbarungen zu einzelnen Anwendungen abschließen zu können, muss ein Überblick bestehen, welche Teile von MS 365 aktiv sind. Ist das unklar, drehen sich BV-Verhandlungen gegenstandslos im Kreis. Aufbauend auf einer Basis-BV, in der die allgemeinen Punkte zusammengefasst werden, soll zu den aktiven Anwendungen die jeweils passende Einzel-BV vereinbart werden.

Damit klar ist, welche Anwendungen überhaupt am österreichischen Unternehmensstandort des deutschen Mutterkonzerns im Einsatz sind, wurde in einer Betriebsvereinbarung festgelegt:



Apps, die nicht in der Anlage aufgeführt sind, sind im Tenant (also in der für das Unternehmen bestimmten Infrastruktur auf den Microsoft-Servern, Anm.) für die Nutzer:innen der österreichischen Standorte zu deaktivieren.

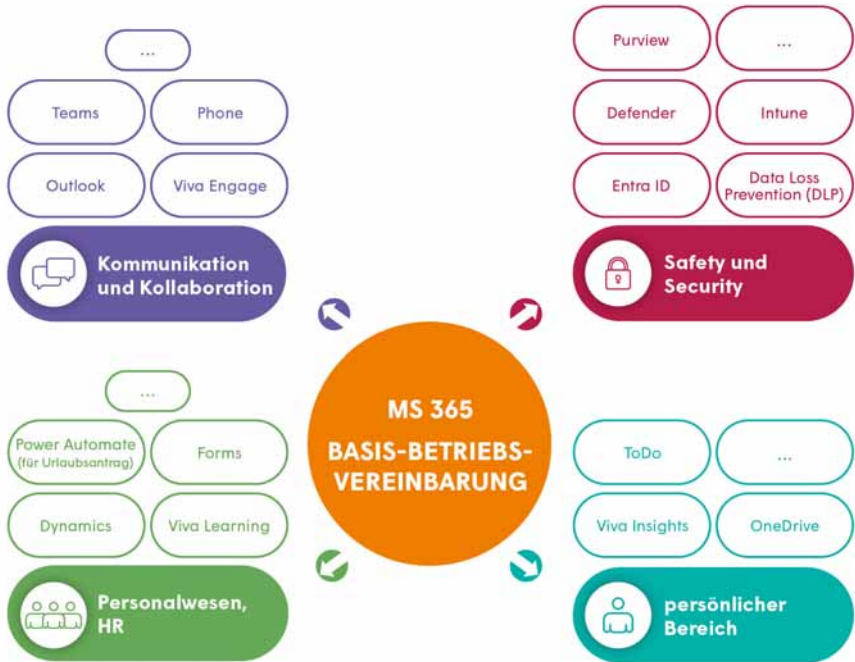
Zusammenfassung der wichtigsten Regelungspunkte in einer Basis-Betriebsvereinbarung zu MS 365

- Rechtsgrundlage nach ArbVG angeben
- Zweck möglichst genau angeben
- Berechtigungskonzept erstellen (= Zugriffskonzept, Rollenkonzept); Einsichts- und Kontrollrechte für den BR festlegen
- Löschkonzept erstellen
- Schulungen anbieten (inkl. Schulung zu privatsphärefreundlichen Einstellungen)
- Auswertungs- und Überwachungsmöglichkeiten beschränken
- Privatnutzung regeln
- Freiwilligkeit festlegen, wo möglich
- Vorgehensweise bei Updates vereinbaren (= Aktualisierungen, Releases, Verbesserungen)
- Ansprechpersonen definieren, MS 365-Gruppe ins Leben rufen

- Vorgehensweise bei Kontrollmaßnahmen bzw. Verdacht auf Fehlverhalten vereinbaren
- Regelmäßige Evaluierung durchführen (inklusive der Risiken für die Privatsphäre sowie der Gesundheitsrisiken)
- Datenschutz-Folgenabschätzung durchführen (gem. Art. 35 DSGVO)

MS 365 deckt ein sehr weites Spektrum an betrieblichen Einsatzmöglichkeiten ab, wobei diese alle eng miteinander verzahnt sind, nicht immer eindeutig voneinander abgegrenzt werden können und mitunter für den Regelbetrieb nicht erforderlich sind. Eine einzelne BV wird daher nicht alles abdecken können und eine BV für jede einzelne Anwendung würde zu einer zu großen Anzahl an BVen führen. Das wäre schnell unübersichtlich und nicht mehr handhabbar. Es ergibt Sinn, eine Struktur einzuführen, die zu den betrieblichen Gegebenheiten passt und die verschiedenen Anwendungen nach Funktionen zusammenfasst; z. B. Kommunikation, IT-Sicherheit, Projektmanagement etc.

Der Überblick und die einzelnen Anwendungen



© Gewerkschaft GPA

© Gewerkschaft GPA

MS 365 bietet *ein* Produkt für alle betrieblichen Anforderungen, *eine* Plattform, *eine* Lösung, *einen* Service – alles kommt aus *einer* Hand. Man kann die verschiedenen Plattformen grob nach Zielgruppen unterteilen, an die sie sich hauptsächlich richten.

1. Jene, die einzelne Nutzer:innen individuell verwenden. Dazu ist beispielsweise **OneDrive** gedacht.
2. Jene, mit denen die verschiedenen Einheiten eines Unternehmens (Abteilungen, Gruppen, Teams, Standorte etc.) zusammenarbeiten. Dazu dient vorwiegend **Teams**.
3. Jene, mit denen die Leitung eines Unternehmens bzw. die damit im technischen Sinne beauftragten Administratorinnen und Administratoren den Ge-

sambetrieb managen, Abläufe festlegen, für Richtlinien sorgen etc. Dazu wird die Plattform **SharePoint** eingesetzt.

4. Die im Hintergrund immer aktiven Safety- und Security-Anwendungen sind auf der Plattform **Defender** zusammengefasst.

Sämtliche Anwendungen sind miteinander verbunden. Die Anwendung, über die sämtliche Daten laufen, heißt **Graph**.

Was Einzelne in ihren persönlichen Bereich stellen, kann so beispielsweise in Teams synchronisiert, also zeitgleich freigegeben werden, und wird außerdem über SharePoint verwaltet, über ein Berechtigungskonzept gesteuert und mittels Anwendungen aus dem Defender auf Sicherheitslücken durchsucht.

Ein und dieselbe Aufgabe kann bei MS 365 mithilfe unterschiedlicher Programme erledigt werden. So kann beispielsweise sowohl das Projektplanungstool Planner als auch ein Channel in Teams (Seite 59) für das Projektmanagement verwendet werden, um Aufgaben zu verteilen oder einen Zeitablauf festzulegen. Um ein Ablesesystem zu verwalten, sind sowohl OneDrive als auch einzelne Channels von Teams (Seite 59) sowie SharePoint (Seite 76) geeignet. Kommunikation kann bei MS 365 auf verschiedensten Kanälen (Chats, E-Mails, Calls, Posts, Lob etc.) über verschiedenste Mittel (Text, Sprache, Bild, Video) stattfinden. Die Vielfalt kann zu Verwirrung führen. Ist ein Kommentar einer Vorgesetzten im Chat ein Vorschlag oder eine Vorgabe? Ist eine neue Aufgabe in Planner eine Anregung oder eine Zuteilung? Muss ein Telefonat über MS Call aufgezeichnet werden oder gilt das nur für Videokonferenzen auf Teams (Seite 59)? Treten derartige Probleme auf, sollte im Unternehmen geklärt sein, welche Kommentare, Beiträge, Posts etc. in welcher Anwendung und von wem gemacht werden sollen, dürfen oder müssen. Ob die Bereiche in den verschiedenen Plattformen und Anwendungen klar voneinander abgegrenzt werden oder ob sie gemeinsam genutzt werden, hängt von den jeweiligen betrieblichen Vorgaben ab – möglich ist (fast) alles.

5 Der Überblick und die einzelnen Anwendungen

5.1 Outlook (= E-Mail, Kalender, Kontakte)

Outlook ist sicher eine der bekanntesten Anwendungen von MS. Mit Outlook verwalten Nutzer:innen Termine, E-Mails, Namen, Adressen und Telefonnummern, Post und Postfächer.

Werden **E-Mails** mit Outlook geschrieben, gelesen, beantwortet und versendet, werden immer auch Verbindungsdaten gespeichert – also Zeitstempel, Betreffzeile, Adressatinnen und Adressaten, Anhänge, Größe, Standort oder IP-Adresse (Internetprotokoll-Adresse ist eine nur ein einziges Mal existierende, mehrstellige Nummer, die dem jeweiligen Gerät im Internet zugeordnet ist, damit es eindeutig erkennbar und erreichbar ist) erfasst. Administratorinnen und Administratoren können diese Verbindungsdaten einsehen (z. B. über MS Purview, Defender (Seite 79) oder eine eigene Office 365 Management-API dafür verwenden). Es ist für zugriffsberechtigte Admins ersichtlich, wer wann welche Betreffzeile an wen versendet hat, wie die Geschwindigkeit der Übertragung war, ob das Datenpaket angekommen ist und ob und wann es geöffnet wurde. Diese Anzeigen für Administratorinnen und Administratoren gehören zum Standard und können technisch nicht abgeschaltet werden – sollen sie auch nicht, weil sonst keine Fehler entdeckt und behoben werden können. Outlook an sich ist also mit einer gewissen Verhaltenskontrolle ausgestattet.

→ **Über den Exchange-Server (das ist der Server von MS, über den die E-Mail-Kommunikation läuft) werden Regeln erstellt, wie mit E-Mails umgegangen werden soll, wie lange sie aufbewahrt werden, auf welcher Basis Spamfilter (also das Aussortieren unliebsamer E-Mails) funktionieren etc. Der Betriebsrat sollte sich die Grundlagen der Aufbewahrungsdauer und der Filter erläutern lassen, um beurteilen zu können, ob sie der unternehmensüblichen Kommunikation entsprechen und um zu vermeiden, dass wichtige E-Mails im Filter hängen bleiben.**

Outlook enthält die Einstellung „Posteingang mit Relevanz“. Ist sie aktiviert, werden „selbstlernend“ „Prioritäten“ für E-Mails erstellt. Anhand der von Nutzer:innen und Nutzern markierten, gelesenen und beantworteten sowie eventuell

mit Fähnchen bewerteten E-Mails (z. B. wichtig/zur Nachverfolgung/erledigt) sowie der hinterlegten organisationsinternen Hierarchien (z. B. Zuordnung zu Abteilungen, Leitungs- oder Assistenzposten) „lernt“ Outlook, welche Absender:innen schnelle Antworten erfordern (z. B. Vorgesetzte) oder welche weniger dringend einer Rückmeldung bedürfen (z. B. wenig finanzkräftige Kundinnen und Kunden). MS ordnet, was für die Nutzer:innen wichtig ist – und was nicht.

Zu E-Mails sollte in der BV geregelt werden:

- **Speicherdauer** festlegen; welche E-Mails werden automatisch aufbewahrt/gelöscht? Welche E-Mails sind individuell, manuell aufzubewahren/zu löschen?
- Überbordende Kommunikation gilt es zu vermeiden, indem **Benachrichtigungen** aus unterschiedlichen Kommunikationstools (z. B. über Statusänderungen) möglichst eingeschränkt oder zumindest stumm geschaltet sind.
- **Vertretungsregelungen** bzw. ein Weiterleitungskonzept festlegen. Wer darf in das Postfach Einsicht nehmen, wenn jemand plötzlich abwesend ist? Welche Vorgehensweise ist bei geplanten Abwesenheiten vorgesehen? Wer vertritt eine abwesende Kollegin oder einen abwesenden Kollegen? Vorgesetzte sollten nur in seltenen und speziellen Fällen E-Mails der Arbeitnehmer:innen sehen oder an andere weiterleiten.



Die Arbeitnehmer:innen sind aufgefordert, bei vorhersehbaren Abwesenheiten automatische Antworten einzurichten. Sollte dies verabsäumt werden, kann die ernannte Vertrauensperson auf Aufforderung der oder des Vorgesetzten eine solche Abwesenheitsnotiz erstellen.

- Privatnutzung festlegen (z. B. eigenes Postfach)
- festlegen, dass der Betriebsrat hinzugezogen werden muss, falls Administratorinnen oder Administratoren Unregelmäßigkeiten oder Auffälligkeiten feststellen.



E-Mails werden grundsätzlich nicht automatisch weitergeleitet. Werden E-Mails aufgrund einer technischen Überprüfung als systemkritisch ein-

Der Überblick und die einzelnen Anwendungen

gestuft, findet keine Übermittlung statt und die betroffenen E-Mails werden vorerst in einem gesonderten Ordner abgelegt und am Ende der darauffolgenden Woche endgültig gelöscht. Die bzw. der Empfänger:in kann sich über den Inhalt des Ordners jederzeit selbst informieren. Sollten vonseiten der Systemadministration E-Mailinhalte eingesehen werden, dürfen die dabei gewonnenen Erkenntnisse nicht zulasten der betroffenen Person verwendet werden.

- Die Einsicht von Administratorinnen und Administratoren begrenzen auf das Vermeiden von Schadsoftware, Angriffen, Datenverlust und ähnlichen Sicherheitsrisiken.



Sollte sich die oder der Systemadministrator:in auf den Arbeitsplatz einer Mitarbeiterin oder eines Mitarbeiters aufschalten müssen, so ist dies nur zur Behebung technischer Probleme nach Zustimmung der Betroffenen möglich.

Der **Kalender** ist ein Bestandteil von Outlook, in dem Termine eingetragen, abgestimmt, an Gruppen versendet oder auch abgesagt werden können. Die Eintragungen werden mitsamt den dazu vorhandenen Informationen wie Ort, Anhängen, Kommentaren, weiteren Teilnehmenden etc. in andere Anwendungen von MS 365 übernommen und können dort dargestellt werden (z. B. als wichtige Themen, wichtige Personen oder als Statusmeldung).

Kalender sollten keine Leistungsvorgaben enthalten (z. B. zehn Kundinnen- bzw. Kundengespräche pro Tag) oder als „Leistungsmesser“ verwendet werden. Kalender sollten nicht als automatische Arbeitszeiterfassung dienen oder mit der Arbeitszeiterfassung abgeglichen werden.

- **Über Exchange (das ist der Server von MS, über den die E-Mail-Kommunikation läuft) kann der Kalender – und dessen Statusanzeigen – für alle (freigeschalteten) Nutzer:innen einsehbar gemacht werden. Kalendereinträge, wer an welchem Ort was mit wem arbeitet, sollten nur für jene Kolleginnen und Kollegen ersichtlich sein, die diese Angaben tatsächlich benötigen.**

- **Beschäftigte können in der Regel über die Einstellungen von Outlook deaktivieren, dass sie Nachrichten aus anderen Anwendungen erhalten oder dass sie Vorschläge für „Fokuszeiten“ von Viva Insights erhalten oder zum LinkedIn-Account automatisch verbunden sind. Die Möglichkeit, das zu deaktivieren, sollte gegeben werden. Eine permanent für alle Beschäftigten eines Unternehmens verfügbare Einsicht in Arbeitszeit und Arbeitsort wäre überschießend.**

Für Kalender sollen in einer BV folgende Punkte geregelt sein:

- Zwecke festlegen (z. B. Terminkoordination, persönliche Monatsplanung)
- Lese- und Schreibberechtigungen möglichst eng begrenzen (wer darf wessen Kalender sehen und Termine ein- und austragen?) und möglichst von den einzelnen Benutzer:innen selbstbestimmt vergeben
- Auswertungsverbot oder eine konkrete Ausnahmeregelung bei anlassbezogenen, begründeten Verdachtsmomenten unter Beteiligung des Betriebsrats
- Speicherfristen festlegen (nach wie vielen Jahren wird ein Kalendereintrag gelöscht? Geschieht das automatisiert?)

5.2 Teams

Nachdem Teams immer umfassendere Einsatzmöglichkeiten erhalten hat, stand der Vorwurf seitens des Mitbewerbers Slack im Raum, MS würde den freien Wettbewerb im Europäischen Wirtschaftsraum beschränken. Die EU-Kommission wurde tätig und leitete im Sommer 2023 ein Verfahren wegen Wettbewerbsverzerrung ein, woraufhin MS kurzerhand Teams von MS 365 entkoppelt hat. Die Plattform Teams ist nun als eigenes Produkt erhältlich und muss nicht mehr im Paket mit anderen MS-Diensten genutzt werden.

Teams kann wesentlich mehr als telefonieren mit Bild. Teams ist zu einer Plattform ausgebaut worden, die sich zum gemeinsamen Bearbeiten und Ablegen von Dateien, zum Versenden von (Chat-)Nachrichten, zur Verknüpfung mit Terminen, Kontakten etc. eignet. Gute Übertragungsqualität und vielfältige Funktionen für

Der Überblick und die einzelnen Anwendungen

verschiedene Medien ohne „lästigen“ Wechsel von einem Format auf ein anderes sorgen dafür, dass MS Teams weit verbreitet ist.

- **Administratorinnen und Administratoren mit der entsprechenden Berechtigung können im „User-Activity-Report“ sehen, welche Personen und/oder welche Gruppen wie viele Chats, Calls, Meetings, Uploads, Downloads usw. getätigt haben.**

Auf Teams können Untergruppen eingerichtet werden, sogenannte **Channels** (z. B. für Projekte oder eine Kleingruppe innerhalb eines Bereichs). Werden auf den unterschiedlichen MS-Anwendungen unterschiedliche Aktivitäten für unterschiedliche Zwecke oder unterschiedliche Gruppen gesetzt, wird es schnell unübersichtlich. Das kann dazu führen, dass Nutzer:innen Dateien nicht mehr auffinden, Dateien auf SharePoint nach wie vor vorhanden sind, obwohl sie „eigentlich“ gelöscht wurden, Dateien keine korrekte Zuordnung oder Klassifikation erhalten etc.

Um Verwirrungen zu vermeiden, muss sorgfältig darauf geachtet werden, wer welche **Berechtigungen** hat und für welche Zwecke Teams verwendet wird. Es sollte daher eindeutig in einer BV dargelegt werden, wozu Teams verwendet wird und wozu es andere Kommunikationskanäle gibt (z. B. für das jährliche Mitarbeiter:innengespräch). Es sollte klar geregelt sein, wer worauf **Zugriff** hat.



Die konkreten Zugriffsrechte werden ausschließlich aufgrund eines entsprechenden IT-Antrags gewährt. Das Zugriffs- und Berechtigungskonzept auf MS-Teams wird als Anlage 1 zu dieser Betriebsvereinbarung genommen. Es basiert auf folgenden grundsätzlichen Bestimmungen:

Der Zugriff erfolgt über personalisierte Login-Daten.

Die Zugriffsrechte für Regionalleiter und den Verkaufsleiter beziehen sich ausschließlich auf die ihnen jeweils zugeordneten Mitarbeiter:innen. Auswertungen für andere Fachbereiche wie z. B. Marketing oder Marktforschung werden ausschließlich in aggregierter Form zur Verfügung gestellt, sodass Rückschlüsse auf einzelne Mitarbeiter ausgeschlossen sind.

Die Spracherkennung

Das **Sprachmodell** von MS (ehem. „Cortana“ genannt) sorgt für die Übertragung von Sprache in Text (z. B. bei Untertiteln zu Videos oder beim Umsetzen eines Sprachbefehls in eine Ausführung) und umgekehrt (liest z. B. einen Text vor). Auch die Übersetzung in andere Sprachen wird – zumindest für häufig gesprochene und geschriebene Sprachen – immer besser und vor allem bei internationalen Treffen gerne genutzt (z. B. im Europäischen Betriebsrat).

Soll eine Aufnahme gemacht werden (Recording), bedarf es meist der vorherigen Information und ausdrücklichen Zustimmung der Teilnehmer:innen. Eine Aufzeichnung von Konferenzen, Gesprächen, Webinaren kann für die spätere Nachvollziehbarkeit sinnvoll sein (z. B. Reklamation bei Dienstleistungen, Entscheidungsfindungen von Gremien), die Einsichtnahme in die Aufzeichnungen sollte allerdings auf einen engen Zweck beschränkt werden (z. B. konkrete Schadensersatzansprüche, Ergebnisse festhalten).

Beim Einsatz von Sprachassistenten im Rahmen von Videokonferenzen mit Teams und beim Recording sollte in einer BV geregelt sein:

- **Verantwortlichkeiten** festlegen; wer überarbeitet? Wer korrigiert (Übersetzungs-)Fehler? Haftungsfragen sollten angesprochen und geklärt werden, so dass die Haftung für fehlerhafte Ergebnisse nicht direkt auf die Arbeitnehmer:innen übertragen wird.
- alle Beteiligten über Verwendungszweck, Empfängerkreise, Aufbewahrungsdauer **informieren**
- die **Zwecke** für allfälliges Aufzeichnen klarstellen (z. B. Protokollierung einer Sitzung, interne Weiterbildung).
- Zielgruppe bzw. **Empfänger:innenkreise** von Aufzeichnungen angeben; für wen wird die Aufnahme zur Verfügung gestellt? Wo wird sie gespeichert? Von wem dürfen Aufnahmen/Chats/geteilte Inhalte auf dem Bildschirm heruntergeladen oder gespeichert werden?
- **Aufbewahrungsdauer**; Wann wird das aufgezeichnete Video gelöscht? Reicht es bei Transkripten und Protokollen, den Originaltext in Echtzeit mitlaufen zu

Der Überblick und die einzelnen Anwendungen

lassen, also nicht zu speichern, oder wird dieser für spätere Überprüfungen gebraucht?

- **Berechtigungs- und Zugriffskonzept**; wer darf Teams-Meetings leiten, Teilnehmer:innen einladen, stumm schalten?
- Die **Rechte am eigenen Bild/Ton/Transkript** klären; in der Regel wird es einer **Zustimmung** zu allfälligen Ton- und Bildaufzeichnungen inkl. Widerrufsrecht bedürfen. Darf transkribiert werden? Von wem muss das Protokoll überarbeitet und freigegeben werden?
- Im Sinne des Arbeitnehmer:innenschutzes sollten hochwertige **Headsets/Kopfhörer** zur Verfügung stehen.
- Sind die Konferenzen länger als eine Stunde, sind **Pausenregelungen** zu treffen (Bildschirmpause)
- Das Ein- und Ausschalten der **Funktionen** bei Teams-Meetings (z. B. Kamera, Mikrofon- und Freigabe von Dokumenten, Hintergrund etc.) sollte so weit als möglich **freiwillig** erfolgen, von den Teilnehmer:innen und Teilnehmern selbstständig aktiviert und deaktiviert werden können.
- **Gesichtserkennung mittels KI** als Standardeinstellung deaktivieren (Achtung: Bei der Aufnahme von Gesichtern handelt es sich um biometrische Daten, und diese unterliegen einem besonderen Schutz und benötigen daher eine Einwilligung der Betroffenen.)

Die Kamera und das Mikrofon

Teams bietet bei der Verwendung der Kamera eine Funktion, die den **Hintergrund** unscharf erscheinen lässt. Diese sollte von den Nutzer:innen und Nutzern besonders dann eingeschaltet werden, wenn sich andere Personen im Raum befinden (z. B. Mehrpersonenbüros, Homeoffice). Sollten weitere Personen ins Blickfeld der Kamera geraten können, müssen diese darüber informiert werden.

Die Verwendung von **Mikrofon und Kamera** kann wie folgt geregelt sein:



Audio- und Videoinhalte können nach vorheriger Information und ausdrücklicher Zustimmung der Teilnehmer:innen der Konferenz durch die

oder den Organisator:in aufgezeichnet werden. Die Aufzeichnung wird jeder und jedem Teilnehmer:in auf dem Bildschirm signalisiert. Eine Aufzeichnung sowie deren Weitergabe oder Bekanntmachung an Dritte außerhalb der teilnehmenden Personen bedarf der vorherigen ausdrücklichen Zustimmung sämtlicher Gesprächspartner:innen. Falls eine Freisprechfunktion genutzt wird, ist die oder der Teilnehmer:in ebenfalls zur Information der im Raum Anwesenden verpflichtet.

Zweck der Aufzeichnung von Konferenzen ist die spätere Nachvollziehbarkeit der Konferenz für Teilnehmer:innen und für Unterrichtende (z. B. bei Webinaren). Unter einer Aufzeichnung sind auch Chatverläufe zu verstehen. Abgesehen von der Aufzeichnung von Webinarinhalten sind Weisungen zu einer verpflichtenden Audio- oder Videoaufnahme unzulässig.

Das Aktivieren der Aufnahmefunktionen durch Dritte ist nicht möglich. Beim Anmelden sowie bei Unterbrechungen und beim Beenden des Programms werden Kamera-, Mikrofon- und Dateifreigabefunktionen der Teilnehmer:innen automatisch ausgeschaltet. Bei aktivierter Kamerafunktion ist die Kamera so auszurichten, dass andere Personen nicht dauerhaft vom Sichtfeld der Kamera erfasst werden. Die bzw. der Teilnehmer:in ist verpflichtet, im Raum anwesende Personen über die aktivierte Kamerafunktion zu informieren. Weisungen zur Verwendung des Livebildes sind unzulässig.

MS Teams bietet für bestimmte Lizenzen auch „**intelligente Kameras**“, die mit KI zur Gesichts- und Spracherkennung ausgestattet sind – das „IntelliFrame“. Dieses Programm kann anhand der Stimme, also eines biometrischen Merkmals, Teilnehmende zuordnen. Es wird also erkannt, wer gerade spricht, und das Bild auf die sprechende Person gezoomt. Ob dieses Feature gebraucht wird, ob der Zweck mit einem gelinderen Mittel erreicht werden kann, muss geprüft und im Unternehmen entschieden werden. Jedenfalls ist zuvor die freiwillige Zustimmung der Teilnehmenden einzuholen, da es sich um besonders schützenswerte Daten von Beschäftigten handelt.

Der Überblick und die einzelnen Anwendungen

Videokonferenzen, Chats und deren Aufzeichnungen sind mittlerweile so **verschlüsselt**, dass MS selbst nicht mehr darauf zugreifen kann. MS bemüht sich hier, Kundinnen- und Kundenwünsche zu erfüllen und die Privatsphäre besser zu schützen.

Kleine Spielelemente

MS 365 bietet „**Lob**“ innerhalb der Teams-Chats in Form von kleinen Bildchen mit einem Löwenkopf (der Mutige), einer Faust (der Problemlöser), einem Basketball (Teamplayer), einem Blumentopf (Wachstum) und weiteren Symbolen an. Die Bilder können als Bewertung der Arbeitsqualität, als Feedback oder auch als „leise“ Kritik gesehen werden. Dabei wird getrackt (also der „Spur gefolgt“), wer wem wann wie oft so ein „Lob“ schickt, wobei die Darstellung ausschließlich Empfängerinnen und Empfängern selbst zur Verfügung steht. Mit der entsprechenden Berechtigung könnten auch Vorgesetzte die „Praise-History“ der Beschäftigten ansehen. Ob diese Elemente der Gamification (also ursprünglich aus der Spielkultur stammendes) im Arbeitsalltag motivieren, ablenken oder demotivieren, ob sie benötigt werden oder nicht, ist abhängig von der Betriebskultur bzw. Geschmackssache.

→ **Die Praise-Funktion kann – je nach Voreinstellung – individuell oder von dazu berechtigten Administratorinnen und Administratoren ausgeschaltet werden.**



(Grafische oder anderwertige) Darstellungen zur Kommunikation innerhalb von Teams sind ausschließlich den Mitgliedern des Teams zugänglich und werden nicht gespeichert, auch nicht exportiert oder in anderen Formaten oder Programmen gespeichert.

Grundsätzlich geht man auf der Teams-Plattform davon aus, dass alle gleichberechtigt darin arbeiten und alle alles sehen. Sollen hingegen online Räume und die darin ausgetauschten Informationen nur bestimmten Personen zur Verfügung stehen, stehen sogenannte „**Channels**“ zur Verfügung.

Ganz ohne Hierarchien geht es auf Teams nicht. Diejenigen, die Teams-Einladungen verschicken oder als „Besitzer“ ausgewiesen sind, erhalten eigene Berechtigungen („special skills“), um Berechtigungen der „normalen“ Teams-Teilnehmer:innen zu moderieren (z. B. Bildübertragung wird allen Teilnehmenden bei großen Zusammenkünften entzogen, um die Übertragungsqualität zu erhalten).



Nur die zuständigen Mitarbeite:innen der IT-Abteilungen legen Teams und Channels an und sind deren Besitzer:innen. Besitzer:innen können auf begründete Anforderung Beiträge löschen.

In Teams können – sofern die Berechtigung dafür vorhanden ist – weitere beliebige Apps aus der Welt außerhalb von MS 365 eingebunden werden. Je mehr Teams, je mehr Channels, je mehr Leseberechtigungen jemandem zugeordnet sind, desto komplizierter wird es und Teams funktioniert nicht mehr ganz so effektiv. Eine Balance herzustellen zwischen Datenintegrität und -stabilität bei gleichzeitiger Aktualität und Richtigstellungsmöglichkeit, zwischen Übersichtlichkeit und Komplexität, zwischen Vertraulichkeit und Transparenz ist eine der größten Herausforderungen.

Die Analysemöglichkeiten

Seit 2020 können Tätigkeiten der letzten sieben bis 90 Tage mit dem **Analysetool** ausgewertet werden. Für „Teams-Besitzer:innen“, also jene, die ein Team angelegt haben, steht mit diesem Tool eine Anzeige zur Verfügung, auf der ein Zeitstempel verrät, wer wie lange an einem Meeting teilgenommen hat, wer das Meeting wie lange verlassen hat oder wer zu spät gekommen ist. Außerdem lässt sich herauslesen, wie oft sich die Gruppenmitglieder austauschen/chatten, wer sich wie häufig zu Wort meldet, und welche Features genutzt werden, wer im letzten Monat wie viele Treffen organisiert, wer an wie vielen Treffen teilnimmt bzw. diese absagt oder wer wie viele Megabyte hochgeladen hat. All das können sich Gruppenleiter:innen bzw. Besitzer:innen im **„Benutzeraktivitätsbericht“** anzeigen lassen.

Anonymität ist in Teams also nur bedingt gegeben. Je kleiner die Gruppe in Teams oder im Channel, desto weniger Anonymität. Daher wird es Schulungen, Informationsarbeit und Betriebsvereinbarungen brauchen, damit diese Daten nicht

zu unlauteren Zwecken eingesehen und verwendet werden und erst recht nicht zu nachteiligen Interpretationen für die Beschäftigten führen.

Für die BV zur Zusammenarbeit auf Teams (Kollaboration) sind folgende Regelungen zu überlegen:

- **Zweck** angeben (z. B. gemeinsame Dateibearbeitung innerhalb einer Projektgruppe),
- Festlegen, wann nicht mehr genutzte Teams, Chats oder Channels (samt allfällig angelegten Dateien/Bibliotheken/Kanälen/Arbeitsräumen/Protokollen/Videos etc.) wieder **gelöscht** werden (z. B. Channel ein Monat nach Projektende; falls Chats nur zum Plaudern dienen, dass sie täglich gelöscht werden).
- Ausführliche **Schulung** als Vorbedingung verankern, die jedenfalls die möglichen Privacy-Einstellungen beinhaltet; insbesondere für jene, die Teams und Channels erstellen.
- **Berechtigungen** festlegen, wer welche Aufgaben in Teams hat. Festlegen, wer die Leitung innehat, wer die Teammitglieder sind, wer Channels anlegt und verwaltet, wer Dateien hinzufügen/verändern/sehen darf.
- **Ansprechperson** bei technischen Problemen festlegen.
- Bestimmen, dass aufgrund der Einsicht in Protokolle/Teilnehmer:innen-Listen usw. **keine Beurteilung** von und **kein Vergleich** zwischen Kolleg:innen erfolgen darf.
- Bei der gemeinsamen **Dokumentenbearbeitung** sollte der Befehl „Steuerung anfordern“ (damit hat die oder der anfordernde Nutzer:in die Möglichkeit, sich als die jeweils andere Person auszugeben und in deren Namen Dokumente zu ändern oder zu löschen) nur bedingt freigegeben werden.
- Der Teilnehmer:innenkreis soll bei einer Dokumentenfreigabe zu jedem Zeitpunkt für jede:n Teilnehmer:in ersichtlich sein (Transparenz und Information).



Für das gemeinsame Arbeiten an Dokumenten, können die Teilnehmer:innen ihren Desktop freigeben, sodass andere diesen sehen können. Die Freigabe des Desktops muss explizit von der oder dem Teilnehmer:in

initiiert und bestätigt werden. „Verdeckte“ Aktionen von anderen Teilnehmerinnen und Teilnehmern sind nicht möglich.

Der Status und der Standort

MS Teams zeigt den „**Status**“ an, ob Kolleginnen oder Kollegen gerade „in einer Besprechung“ oder „in einem Call“ sind, was aufgrund des Terminkalenders (Seite 56) oder der aktiven Telefonfunktion festgestellt wird. Der Status kann nicht nur in Teams, sondern auch in anderen Anwendungen angezeigt werden (z. B. Viva oder Outlook). Um stets korrekte Informationen zu liefern, müssten Nutzer:innen ihren Status immer angeben, Termine im Kalender akkurat einhalten und sämtliche Telefonate über MS führen. Es fragt sich, ob permanente Statusanzeigen im Arbeitsalltag hilfreich sind und ob es nicht ein gelinderes Mittel gibt, um jemandes Erreichbarkeit festzustellen.

Seit Oktober 2024 offeriert MS 365 die Option, **Standort und Arbeitszeiten** freizuschalten und somit in Teams (Seite 59) sowie über den Kalender von Outlook anzuzeigen, wer gerade wo im Bürohaus ist und wer auf Telearbeit. Seit August 2026 steht eine Anwendung namens „**Places**“ zur Verfügung, die den Standort bereits mit dem Einloggen ins firmeneigene WLAN erfasst. Damit sollen die Buchung eines Schreibtisches im Großraumbüro, das Reservieren eines Konferenzraumes samt dazugehöriger Ausstattung, die Auslastung der Räumlichkeiten eines Standorts etc. ermöglicht werden. Damit wäre der Standort von Kolleginnen und Kollegen in der Firma ersichtlich. Bei freundlicher Interpretation könnte man das nutzen, um sich neben den Lieblingskollegen zu setzen, bei unfreundlicher dazu, Personen zu diffamieren.

→ **Soll der Arbeitsort sowie der Präsenzstatus in Teams generell deaktiviert werden, braucht es eine:n Administrator:in, die oder der im „Employee Center“ die jeweiligen Profile abändern kann, sodass entweder die Anzeige „permanent offline“ bleibt oder der „Privacy Mode“ aktiviert ist. Im „Privacy Mode“ bestimmen Nutzer:innen selbst, welcher Status für Kolleginnen und Kollegen angezeigt wird. Der Präsenzstatus lässt sich dauerhaft auf „offline“ stellen. Diese Möglichkeit sollte im Admin-Cen-**

Der Überblick und die einzelnen Anwendungen

ter freigegeben werden, damit individuell gewählt werden kann, welcher Status angezeigt wird.



Die Verwendung des Status bzw. der Präsenzinformation ist freiwillig und kann von der oder dem Benutzer:in jederzeit manuell geändert werden. Weisungen zur Verwendung des Status sind unzulässig.

Die in einigen Modulen vorzufindende Verfügbarkeitsanzeige einer Mitarbeiterin oder eines Mitarbeiters darf weder zum Zweck der Zeiterfassung noch zur Kontrolle verwendet werden, ob Arbeitszeiten, Ruhepausen und Ruhezeiten eingehalten werden.

Status lassen keine objektiven Rückschlüsse auf das Verhalten der dahinterstehenden Personen zu und sind daher nicht auszuwerten. Die Information zum Status ist für eine Bewertung von Arbeitsleistungen nicht geeignet und darf dafür nicht genutzt werden.

Zusammenfassung, was in einer BV zu Statusanzeigen und „Places“ geregelt sein soll

- **Freiwilligkeit** von Statusanzeigen
- **Reine Echtzeiterfassung**, keine Speicherung oder Auswertung
- Deaktivierung der Möglichkeit, andere Nutzer:innen über Statusänderungen zu benachrichtigen
- **Auswertungsverbot** für Analysen, deren Zweck es ist, individuelles Verhalten zu vergleichen oder zu beurteilen
- Status als Arbeitszeiterfassungsinstrument untersagen

Zu den jeweiligen Nutzungsmöglichkeiten von Teams hat man sich in einer BV auf folgende Löschregelungen geeinigt:



Chat – Benutzer:innen können ihre Nachrichten ändern und löschen, Teams-Besitzer:innen können auf begründete Anforderung Beiträge löschen.

Video – Liveanzeige bei anderen Videotelefonie-Beteiligten, Aufzeichnung nur von Live-Events nach separater Freigabe durch den Betriebs-

rat, Zustimmung der Betroffenen und expliziter Definition der Löschfrist.

Dokumentenablage – gemeinsame Ablage für Teams, Abteilungen, Gesellschaften, den gesamten Konzern, mit registrierten Gästen, Löschung nach dem Event mit Gästen, Löschung von Besitzerinnen und Besitzern bei internen Channels.

Zusammenfassung für gute Voraussetzungen für die Nutzung von Teams:

- an die jeweils aktuellen Arbeitsaufgaben angepasstes **Berechtigungsmanagement** (sonst haben die Beschäftigten veraltete oder fehlende Zugriffsberechtigungen)
- strukturiertes **Dokumentenmanagement** inklusive Archivierung und Löschprozessen (sonst wird es unübersichtlich, welche Dateien die aktuellen bzw. die richtigen sind und wo sie zu finden sind)
- eindeutiges **Meetingmanagement** (sonst werden zu viele Termine/Meetings/Anfragen gestellt und die Erwartungshaltung an ständige Erreichbarkeit wird überbordend)
- klare Einteilung und **Abgrenzung** der Teams und Channels je nach Verwendungszweck und Zielgruppe (sonst kommt es zu Doppelungen)
- Filtern oder **Deaktivieren** der Benachrichtigungen innerhalb der verschiedenen Teams, Channels, Chats und Outlook (sonst kommt es zu einer Flut an Benachrichtigungen)
- **Zuständigkeiten** für die verschiedenen Teams/Channels klären (sonst ist es kaum möglich, den Überblick zu bewahren sowie verpflichtende von freiwilligen Aktivitäten zu trennen)
- **Schulungen** (sonst erkennen Nutzer:innen den Sinn nicht und es fehlt an Akzeptanz)
- **Datenschutz** und Compliance (sonst entstehen (Sicherheits-)Lücken, wodurch Transparenz und Vertraulichkeit verloren gehen)

Der Überblick und die einzelnen Anwendungen

- Schnittstellen-Management (sonst können beliebig viele Apps eingebunden werden, was zu Verwirrung führt)

5.3 Copilot und Agents – die KI bei MS 365

Die bekannteste Künstliche Intelligenz (KI), die derzeit sowohl gratis als auch als Bezahl-Version verfügbar ist, stammt von dem Unternehmen **OpenAI** und heißt **ChatGPT**. GPT steht für „Generative Pre-trained Transformer“, frei auf Deutsch übersetzt in etwa „schöpferischer/kreativer angelernter Überleiter“. Microsoft investierte 2019 über eine Milliarde Dollar in die Entwicklung von ChatGPT¹⁵, also über 875,820,000 Euro. 2023, als die Welt das Licht von ChatGPT erblickte, schob Microsoft zehn Milliarden Dollar nach. MS hält (derzeit) 27 Prozent Anteile in der Stiftungsstruktur¹⁶ und ist (derzeit) zu 20 Prozent am Umsatz beteiligt.¹⁷ OpenAI betreibt die meisten seiner Angebote in der Azure Cloud, die wiederum MS gehört. Die Unternehmen sind also eng miteinander verflochten. Kürzlich wurde die ziemlich exklusive Partnerschaft gelockert, OpenAI baut den profitablen Geschäftszweig aus und bietet seine KI auch in der Cloud von MS-Konkurrenz an (z. B. Google, Oracle).

MS hat seit 2024 jede Menge KI, basierend auf dem KI-Modell von ChatGPT, unter dem Namen **Copilot** in seine Anwendungen eingebaut. Im Dezember 2024 musste für eine Copilot-Lizenz noch um 22 Euro pro Nutzer:in zugekauft werden. Mittlerweile (Sommer 2026) sind über 80 Copilots – teilweise standardmäßig – in die Welt von MS 365 integriert.¹⁸

Copilots bauen auf dem KI-Modell von ChatGPT auf, das menschliche Sprache verarbeitet und gesprochener Sprache sehr ähnliche Antworten generiert. Es arbeitet nach der Wahrscheinlichkeitsrechnung. Im Satz folgt also jenes Wort, welches – gemessen am Trainingsmaterial – am wahrscheinlichsten passt. Bei Anfragen zur Programmierung wird jener Code ausgewiesen, der am wahrscheinlichsten zum angestrebten Ziel führt. Bei Bilderstellung wird das geliefert, was wahrscheinlich gewünscht ist usw. Copilot erstellt Zusammenfassungen, Transkripte, Recherchen, Fehlersuche, Übersetzungen, Prioritäten, Vorschläge, Bilanzen, Programmiercodes, Gedichte, Bilder, Hausübungen, Zeitungsartikel, Videos. Klingt

nach viel? Ist auch viel. Manches davon sollte der Hausverstand verhindern – wie beispielsweise das Publizieren von Rechtskonformitätsberichten.¹⁹

Copilot kann sowohl auf unternehmensinterne Daten begrenzt sein (z. B. zur Priorisierung von Aufgaben im Kalender) als auch ausschließlich mit Internet verfügbarem Material arbeiten (z. B. in der Suchmaschine Edge) oder beide Welten miteinander verknüpfen.

Bei der Arbeit mit internen Copilots wird die Anfrage (der Prompt) zuerst mit Informationen aus MS Graph verarbeitet. Mittels Graph werden Daten aus verschiedenen MS 365-Quellen bereitgestellt (z. B. E-Mails, Dateien, Kalendern etc.). Daraufhin wird die Anfrage an das KI-Modell gesendet, das Open AI entwickelt hat. Das Unternehmen OpenAI hat laut MS keinen Zugriff auf die Daten, da diese innerhalb der von MS betriebenen Cloud-Infrastruktur Azure ausgewertet werden. Die fertige Antwort von Copilot wird in der letzten Bearbeitungsschleife durch unternehmensinterne Richtlinien geprüft (Compliance und Governance). Auf diese Weise generiert Copilot „kontextbezogene und personalisierte Antworten, während gleichzeitig Datenschutz und Sicherheitsstandards eingehalten werden“, so MS. Nicht immer scheint das zu gelingen, findet man schließlich im Internet mittlerweile seitenweise Anleitungen, wie Copilot geschickt zu seltsamen Antworten gebracht werden kann.

Eine versierte IT-Abteilung kann selbst „**Agenten**“ mittels Copilot erzeugen – oder die standardmäßig von MS bereitgestellten verwenden. Copilot Agents werden eingesetzt, um spezifische Aufgaben zu automatisieren (z. B. routinemäßige Datenanalysen erstellen, Chatbots für Kundinnen- und Kundenanfragen, Weiterleiten von Tickets an die zuständige Person, Programmcode testen und Ähnliches). Einem Agent kann vorgegeben werden, in welchem Stil zu antworten ist, welche Abläufe zu befolgen sind oder auf welche Dokumente *nicht* zurückgegriffen werden soll (beispielsweise die als „top secret“ klassifizierten).

MS meint, dass Agent insbesondere im HR-Prozess nützlich sind und nennt als Beispiel: „Mitarbeiterumfragen entwerfen, Umfragen analysieren, um wertvolle Einblicke in die Stimmung der Mitarbeiter zu gewinnen.“ Ein Agent liefere eine „wertvolle Kennzahl zur Beurteilung des Mitarbeiterengagements [sic!]. Sie [die

Der Überblick und die einzelnen Anwendungen

Kennzahl] misst, wie wahrscheinlich es ist, dass Ihre Mitarbeiter Ihr Unternehmen ihren Freunden oder ihrer Familie als großartigen Arbeitsplatz empfehlen". Engagement wird von MS an Empfehlungen in der Privatsphäre gemessen. Das zeigt, wie wenig MS den Schutz der Privatsphäre berücksichtigt und wie stark Emotionalisierung im Vordergrund steht.

Mit dem zunehmenden Einsatz von KI lassen sich Auswertungen über Beschäftigte deutlich schneller und einfacher erstellen als noch vor einigen Jahren. Dabei darf nicht vergessen werden, dass KI auf Wahrscheinlichkeitsberechnungen basiert, dass KI von Grund auf eine Verzerrung durch die Ausgangsdaten inneohnt und dass zahlreiche rechtliche Fragen wie Urheberschutz und Haftung (noch) offen sind. Die praktische Anwendung ist also keineswegs fehlerfrei und rechtssicher. MS selbst weist auf seinen Webseiten zu Copilot – ebenso wie bei anderen Anwendungen mit KI – immer wieder darauf hin, dass die Ergebnisse fehlerhaft sein können und zu überprüfen sind, bevor sie veröffentlicht werden.

- **„Please review data before publishing“ (Deutsch: Bitte die Daten vor der Veröffentlichung überprüfen.)** liest man häufig auf den einschlägigen Webseiten zu KI von MS, und das ist ernst zu nehmen. Im Unternehmen muss klargestellt werden, wie mit den von Copilot (oder einer anderen KI) generierten Ergebnissen umzugehen ist.
- **Empfohlen ist eine Anwendung von Copilot erst nach einer Testphase, bei der die zukünftigen Nutzerinnen und Nutzer sowie der Betriebsrat eingebunden sind.**

Einige wichtige Fragen zwischen Betriebsrätinnen bzw. Betriebsräten und Geschäftsführung sollten beantwortet und in einer Betriebsvereinbarung geregelt sein, wenn Copilot zum Einsatz kommt:

- Für welche **Zwecke** soll Copilot verwendet werden? (z. B. Erstellen von Protokollen nach Teams-Sitzungen).

- Gibt es Aufgaben, für die Copilot **keinesfalls** eingesetzt werden darf? (z. B. Zusammenfassung von als „streng vertraulich“ klassifizierten Dokumenten) Gibt es Daten, Unterlagen, Aktivitäten von Personen, die aus den Berechnungen **ausgeschlossen** werden sollten oder aufgrund rechtlicher Geheimhaltungspflichten ausgenommen werden müssen?
- Ändern sich die Anforderungen an **Qualifikationen** von Arbeitnehmerinnen und Arbeitnehmern? Erfordert die Korrektur der Ergebnisse und Vorschläge von Copilot spezielle Kompetenzen? Braucht es dazu eigene Schulungen? Wurden die Nutzer:innen für die Anwendung geschult? Erfolgt die Schulung bzw. das Ansehen von Schulungsmaterial (z. B. YouTube-Videos) während der Arbeitszeit? Hier sollte sich der Betriebsrat die Teilnahme an den Schulungen ausbedingen, die nicht auf seine Bildungsfreistellung gemäß § 118 ArbVG angerechnet werden.
- Ist die Verwendung von Copilot **freiwillig**? (Natürlich ist juristisch im Arbeitsverhältnis kaum Freiwilligkeit gegeben und technisch fließen die Daten der Beschäftigten in der Regel in den Copilot mit ein, dennoch sollte geklärt werden, ob er verwendet werden muss. Und wenn „ja“: von wem und wofür?) Oder ist er verpflichtend zu verwenden (z. B. als Prüfinstrument vor dem Fertigstellen von Code)? Sind die Ergebnisse als Vorschläge verpflichtend umzusetzen (z. B. Prioritäten bei Antworten auf E-Mails)?
- Wer ist **verantwortlich** für Ergebnisse, die mit Copilot erstellt werden? Hier sollte jedenfalls auf das Dienstnehmerhaftpflichtgesetz verwiesen werden und die Verantwortung nicht an Arbeitnehmer:innen „durchgereicht“ werden.
- Müssen Ergebnisse eigens **gekennzeichnet**, also als mit KI erstellt ausgewiesen werden (z. B. mit einem Vermerk „Diese Präsentation wurde mit Hilfe von Copilot erstellt“)?
- Ändern sich die **Arbeitsaufgaben**? Werden Arbeitsaufgaben durch Copilot ersetzt?
- Wie und an welcher Stelle ist der **Betriebsrat eingebunden**?

Der Überblick und die einzelnen Anwendungen

- Gibt es eine oder besser mehrere eigens qualifizierte Personen im Unternehmen, die für Fragen der Anwender:innen zur Verfügung stehen (z. B. **Copilot-Expertin bzw. -Experte**)?
- Ändern sich Anforderungen an die **Datenqualität** im Unternehmen? Müssen eigens Daten eingegeben oder korrigiert werden, damit Copilot Ergebnisse erzielen kann? Wer ist verantwortlich für die allenfalls erforderliche Klassifizierung, die Zuordnung der Dateien?

5.4 Anwendungen für IT-Administratorinnen und -Administratoren (Backend)

Dieses Kapitel wendet sich jenen Anwendungen von MS 365 zu, zu denen einzelne Nutzer:innen in der Regel keinen direkten Zugriff haben. Sie dienen dazu, das Gesamtsystem MS 365 am Laufen zu halten, Fehler zu entdecken, korrigierend einzugreifen, Verlorenes wiederzufinden, die IT-Sicherheit zu gewährleisten, Berechtigungskonzepte einzurichten usw. Zu ihnen hat üblicherweise nur jemand mit entsprechender Ausbildung Zugang, also eine Administratorin oder ein Administrator.

Die **Vergabe der Berechtigungen** (auch „Rollen“ genannt) ist das Um und Auf des sicherheitstechnischen Datenschutzes. Wer worin Einsicht nehmen darf, wer welche Anzeigen sehen darf (lesende Rolle), wer welche Änderungen vornehmen kann (schreibende Rolle), das muss im „Backend“, also im digitalen Hintergrund, in der Systemverwaltung, eingestellt werden. In den Admin-Centern von Teams, SharePoint, Exchange oder Purview wird das jeweilige Konzept erstellt. Diese Aufgabe kann je nach Unternehmensgröße und -struktur äußerst komplex werden. MS stellt verschiedene Anwendungen zur Verfügung, um ein Zugriffs- und Berechtigungssystem aufzubauen (z. B. Identity Manager, Conditional Access, Single Sign On, Shared Account Password Rollover, BitLocker, Multifaktor Authentication u. a.).

→ **Privilegierte Nutzerrechte, also Berechtigungen für heikle Programme, sollten immer nur an „echte“, natürliche Personen im Betrieb vergeben**

werden, also nicht an Gruppen oder Funktionen (z. B. `service@betrieb.at` oder `helpdesk@betrieb.at` sollen kein Zugriffsrecht auf sensible Security-Programme erhalten).

- An Führungskräfte sollten keine Admin-Rechte vergeben werden (Ausnahme ist die IT-Abteilung), damit diese sich keine personenbezogenen Auswertungen ansehen können.
- Es können (lesende) Einsichtsrechte an Betriebsrätinnen und Betriebsräte vergeben werden (z. B. um zu prüfen, ob sich Beschäftigte und Führungskräfte an die Vertretungsregeln in Outlook halten).

Mit „role based access control“ (RBAC) kann theoretisch jede beliebige Zugriffs- und/oder Leseberechtigung erstellt werden. Sie kann dazu verwendet werden, Beschäftigte von bestimmten – oder auch sämtlichen – Anwendungen, Dateien oder Kommunikationsmitteln auszuschließen. Aus Security-Gründen kann das erforderlich werden, um beispielsweise Virenverbreitung zu unterbinden. Sollte das allerdings als Disziplinarmaßnahme eingesetzt werden, ist die Mitsprache des Betriebsrats zuvor zu garantieren.



Setzt die IT-Abteilung personenbezogene Maßnahmen, die den Zutritt von Beschäftigten zu deren Arbeitsmitteln einschränken oder gar verhindern, ist der Betriebsrat hinzuzuziehen. Muss die Maßnahme aufgrund von Gefahr im Verzug sofort getroffen werden, ist der Betriebsrat unmittelbar im Nachhinein zu informieren, ihm die Gefahr darzulegen und weitere Folgen oder die Zurücknahme der Einschränkung mit dem Betriebsrat zu vereinbaren.

5.5 Graph

Graph kann man sich als das „Herz“ oder auch das „Hirn“ (oder beides zusammen) von MS 365 vorstellen. In Graph werden sämtliche Aktivitäten, Dateien, Metadaten, Inhaltsdaten usw. aus allen anderen MS 365-Anwendungen zusammengeführt. Graph ist die „Zentrale“, die „weiß“, wer, wie lange, wie häufig, mit wem,

Der Überblick und die einzelnen Anwendungen

mit welchen MS 365-Anwendungen arbeitet. Graph speichert Telemetriedaten nicht selbst, sondern greift auf andere Anwendungen zurück und stellt die Ergebnisse wiederum anderen zur Verfügung, wobei durch Graph die Daten sozusagen für andere Anwendungen gefiltert werden. Graph stellt die Beziehungen zwischen den riesigen Datenmengen der MS 365-Welt her.

Über Schnittstellen (Graph Connectors) können Apps außerhalb von MS 365 integriert werden.

- **Die permanente Datenverarbeitung durch Graph läuft immer. Graph kann man nicht deaktivieren. Graph kann man nicht direkt auslesen. Umfassende technische Verhaltens- bzw. Aktivitätskontrolle wohnt dem System von MS 365 durch den Aufbau, die Architektur, fix inne.**

Für die BV zu regeln:

- Allfällig vorhandene Schnittstellen zu anderen Programmen (Application Programming Interfaces, API) außerhalb der Welt von Microsoft, die mit personenbezogenen Daten von Beschäftigten arbeiten, sollten definiert und nur für festgelegte Programme und eindeutige Zwecke genutzt werden.

5.6 SharePoint

SharePoint ist ein zentraler Bereich, über den die MS 365-Anwendungen verwaltet werden. Über SharePoint werden Benutzer:innen hinzugefügt und entfernt, Seiten eingerichtet, Dokumente und der Zugriff darauf verwaltet usw. SharePoint ist ein riesiges Content-Management-System (CMS), auf dem unterschiedlichste Formate eingehängt werden können.

Welche Daten in dieser mächtigen „Schaltzentrale“ verwendet werden, wurde in einer Betriebsvereinbarung folgendermaßen transparent gemacht:



Neben den aus Entra ID importierten Benutzerdaten werden folgende Arbeitnehmerdaten durch das System verarbeitet:

1. Ersteller-/Bearbeiterdaten/Zeitstempel von Dokumenten

2. Organisator-/Teilnehmerinformationen bzgl. Terminen in Kalendern
3. Präsenzinformationen
4. Dokumentenmanagement mit Dokumentenhistorie
5. Tasklisten in Teamspace
6. Freigabefunktion zur Beantragung einer Teamspace-Freigabe von Dokumenten

Es werden auf Personenebene keine Auswertungen oder Reports über das Nutzerverhalten erstellt. Auswertungen über das objektbezogene Nutzerverhalten (z. B. Anzahl von Klicks pro Seite) können auf anonymisierter Basis durch Key User und Systemadministratoren erfolgen.

Jedes Unternehmen, das MS 365 nutzt, sollte einen Prozess durchlaufen haben, der klärt, wie Seiten, Dokumente und anderer Inhalt (Content) auf SharePoint erstellt, genehmigt und genutzt werden dürfen. Andernfalls sind Verwirrung, Doppelgleisigkeiten, Wissensverluste und ähnlich unangenehme Vorkommnisse vorprogrammiert. SharePoint sollte nur von gut dafür geschulten Personen eingerichtet werden. Diese „Seitenbesitzer“ (auch „Owner“ genannt) einer SharePoint-Seite haben nämlich Zugang zu personenbezogenen Protokollen (Logfiles), sehen also sämtliche Aktionen von Nutzerinnen und Nutzern auf „ihrer“ Seite. „Als Websitebesitzer können Sie steuern, ob Personen die Namen von Personen sehen, die Dateien oder Seiten auf einer Website anzeigen“, schreibt Microsoft. Beschäftigte sollten sich dessen bewusst sein und davor geschützt werden, dass ihre Nutzungsaktivitäten beliebig verfolgt (getrackt) werden.



Auf der SharePoint-Einstiegsseite wird dargestellt, wer zum Benutzer:innenkreis zählt und wer Hauptverantwortliche:r, also „Owner“, der SharePoint-Seite ist (z. B. Betriebsrat).



Aktivitätsberichte werden ausschließlich in anonymisierter Form im Admin Center dargestellt. Im Admin Center stehen dem Service Provider anonymisierte Berichte zur Verfügung, wie z. B. Microsoft-Browserverwendung, E-Mail-Aktivitäten, Teams-Nutzungsaktivität. Standardmäßig werden Benutzerdetails für alle Berichte ausgeblendet (...).

Aktivitätenprotokolle könnten – so ein von MS angeführtes Beispiel – nach jenen Arbeitnehmerinnen und Arbeitnehmern gefiltert werden, die demnächst das Unternehmen verlassen. Diese werden dann dahin gehend untersucht, ob sie sensible Informationen eingesehen, Daten heruntergeladen, Dateien mit Personen außerhalb des Unternehmens geteilt, in großem Umfang ausgedruckt usw. haben. MS tut dies unter dem Gesichtspunkt, Datendiebstahl hintanzuhalten, berücksichtigt dabei aber nicht, dass alle scheidenden Beschäftigten durch diese Auswertung einem Generalverdacht ausgesetzt sind. Unbedacht bleibt ebenso, dass die Auswertung in die andere Richtung gemacht werden könnte, also aus bestimmtem Verhalten abgeleitet wird, wer den Betrieb verlassen könnte. Fehlinterpretationen wäre damit Tür und Tor geöffnet und bestimmte Beschäftigte könnten unter einen Generalverdacht geraten, Rechtfertigungsdruck spüren, diskriminiert werden oder Ähnliches.

Das Anzeigen namentlicher Benutzer:innenaktivitäten ist im Protokoll des Purview-Compliance-Portals ersichtlich und kann folglich ausgewertet werden. Die Bedingungen für eine Auswertung von Benutzer:innenaktivitäten sollten jedenfalls gut überlegt und vereinbart werden.



Unter Einbindung des Betriebsrates kann im Bedarfsfall, also bei einem schwerwiegenden und begründeten Verdacht auf Fehlverhalten Einzelner, ein Zugriff auf Benutzerdaten angefordert werden; eine sogenannte „eDiscovery-Sitzung“ wird seitens der IT-Securityabteilung oder der Abteilung für interne Revision mit den dafür eindeutig definierten Beteiligten abgehalten.

In der BV sollte geklärt werden:

- **Berechtigungskonzept:** Wer hat welche Berechtigung? Wer darf eine SharePoint-Seite einrichten? Wer darf Änderungen vornehmen? Wer darf welche SharePoint-Seite einsehen? Wer darf Auswertungen machen?
- Eindeutige **Zwecke**, wozu welche Sharepoint-Seiten verwendet werden dürfen, sowie Festlegung, welche Daten nicht auf bestimmten SharePoint-Seiten abgelegt werden sollen

- Festlegung, wie viel **Speicher** für wen auf welchen Seiten zur Verfügung steht, und die Nutzer:innen darüber informieren.
- **Löschkonzept**
- **Schulungen** für Anwender:innen
- **Einsichtsrechte** für den Betriebsrat regeln (bei Bedarf eine eigene SharePoint-Seite für den Betriebsrat einrichten).
- Allfällig eingebundene externe Anwendungen und **Schnittstellen** darstellen und den jeweiligen Zweck bestimmen.
- Nutzer:innenverhalten ohne Personenbezug (also anonym) analysieren und nur einem engen Personenkreis für einen konkreten Anlassfall zugänglich machen.
- Folgemaßnahmen bei festgestelltem Fehlverhalten nur in Absprache mit dem Betriebsrat.

5.7 Purview und Defender

Mit dem Update von Jänner 2023 erhielten Safety- und Security-Anwendungen von MS den Vornamen: Purview (Deutsch: Einfluss- oder Zuständigkeitsbereich). MS Purview ist eine Plattform für Datenverwaltung und Datensicherheit. Sie umfasst – je nachdem, wie sie im Betrieb zusammengestellt wurde – verschiedene Anwendungen zur Datensicherheit und zur Minimierung von Compliance-Risiken, kurz: dem Datenmanagement. Mit den Anwendungen auf Purview kann man Abweichungen von „normalen“ Verhaltensweisen feststellen, Alarm auslösen, auffälliges Verhalten unter „Quarantäne“ stellen, also vom übrigen System isolieren, damit kein (weiterer) Schaden angerichtet werden kann, Sicherheitslücken schließen und Gefahren mittels KI-Anwendungen vorhersagen.

Eine der meistverwendeten Anwendungen ist der Purview **Defender** (Deutsch: Verteidiger). Dieser dient, wie der Name unschwer erkennen lässt, der Abwehr von Schadsoftware (z. B. Viren, Würmern, Trojanern, offenen Hintertüren). Im Admin-Center von Purview (Compliance-Portal) werden die Regeln festgelegt, welche Aktivitäten als Bedrohung gelten und wann ein Alarm ausgelöst wird (z. B.

Der Überblick und die einzelnen Anwendungen

wenn ein Passwort dreimal hintereinander falsch eingegeben wird oder wenn ein:e nicht verifizierter Nutzer:in mehrmals hintereinander eine E-Mail öffnen möchte oder wenn jemand aus dem Unternehmen auf verbotenen Internetseiten surft usw.). Es wird protokolliert, was vor einem Vorfall, also einem Alarm, passiert ist, um daraus zukünftige zu vermeiden, und es wird festgelegt, wie auf einen Alarm reagiert wird (z. B. Passwörter zurücksetzen, Anmeldevorgänge blockieren, E-Mails löschen etc.), sodass einem abermaligen, ähnlichen Ereignis möglichst vorgebeugt wird. Was als Gefahr für die Compliance und die Sicherheit gilt, ist sehr weit gefasst und reicht von unangemessener Sprache und Beleidigungen über das Erkennen von kompromittierten Nutzerkonten und unerwünschten Applikationen, Offenlegung von vertraulichen Dokumenten gegenüber nicht autorisierten Personen bis hin zum Aufdecken von (beabsichtigter und bevorstehender) Sabotage, Insiderhandel, Korruption und Geldwäsche.

→ **Eine Absprache mit dem Betriebsrat, was in Purview Defender als Sicherheitsrisiko definiert ist, empfiehlt sich.**

Für diese permanente Kontrolle werden die Inhalte von E-Mails, Chats, Dateien usw. der Nutzer:innen eingeordnet. Die Regeln (Englisch: communication compliance) können den vorgegebenen Standardeinstellungen folgen und/oder zusätzlich unternehmensintern definiert sein. Sie können mit einer Historie ausgestattet werden (trainable classifiers definition) sowie mit „Künstlicher Intelligenz“ ergänzt werden, sodass eine durchaus extensive Überwachung die Folge sein kann.

→ **Mit der Berechtigung „Microsoft Configuration Manager (ConfigMgr)“ können Berichte darüber angesehen werden, ob Defender Sicherheitslücken gefunden hat (z. B. ob alle mobilen Geräte im Unternehmen die letzten Updates erhalten haben). Defender listet auf, von welchen Geräten ein besonders hohes Gefahrenpotenzial ausgeht und schlägt vor, wie das Problem behoben werden kann (Recommended Action). Der Betriebsrat könnte sich hin und wieder einen solchen Bericht zeigen lassen und Vorschläge zur Problembeseitigung einbringen.**

Der Defender kann für Bildungsmaßnahmen eingesetzt werden, mit dem Ziel, die Beschäftigten für Security-Probleme zu **sensibilisieren**. Dabei werden Bedrohungsszenarien anhand der vorhandenen Daten entwickelt. Es wird mithilfe des Defender ein Cyber-Angriff simuliert, der etwa damit beginnt, dass eine Massen-E-Mail mit der Betreffzeile: „Sie haben im Lotto gewonnen“ verschickt wird. Öffnen Beschäftigte Anhänge (Englisch: Attachments) solcher E-Mails (Phishing-Mails), die, wenn sie von echten Angreifern verschickt werden, meist Viren enthalten, sendet in unserem Szenario Defender ein weiteres gefälschtes E-Mail (Fake-E-Mail) an jene Beschäftigten, die als Risiko identifiziert wurden. Die Adressatinnen und Adressaten erhalten so die Gelegenheit, ihre Reaktion zu verbessern, sprich: die Anhänge nicht zu öffnen. So sollen die Nutzer:innen lernen, zukünftigen Schaden zu vermeiden. Angriffsszenarien sind mittlerweile sehr fortgeschritten und erfolgen mittels Anrufen von echten Menschen, scheinbar harmlosen Links bis hin zu KI-generierten Chatbots, die Stimmen bekannter Personen nachahmen oder die typische Schreibweise und Firmenlogos imitieren (sogenannte Deep-Fakes). Dementsprechend können auch die (verdeckten) betriebsinternen Übungen ausgefeilt sein. Mitunter werden diese Intrusion-Tests an externe Firmen übergeben, die dann die – im Fall des Falles erforderliche – Schulung mit anbieten.

MS bietet mehrere **KI-Systeme** (z. B. Copilot Defender, Azure Copilot oder Copilot Security), die im Voraus erkennen sollen, ob, wodurch und wo genau Gefahren drohen; es geht etwa um gehackte Anmeldedaten, betrügerische E-Mails, Schadsoftware und Ähnliches, das erkannt und abgewehrt werden soll.

Für den Defender und die darin erstellten Aktivitätsprotokolle, Kriterien für einen Alarm oder erkannte Schulungs- und Gefahrenpotenziale ist in einer Betriebsvereinbarung zu regeln:

- **Einsichtsrechte**; wer die Aktivitätsprotokolle sehen darf
- Wie der **Betriebsrat** eingebunden wird, wenn **Sicherheitsvorfälle** passieren
- Wie die **Information** der Beschäftigten erfolgt (z. B. über Sicherheitsstandards, richtiges Verhalten und allfällige Folgen von Sicherheitslücken)

Der Überblick und die einzelnen Anwendungen

- Wie mit Kontrollen/**Tests** des Verhaltens der Nutzer:innen umzugehen ist
- Welche Folgen das Verhalten der Beschäftigten bei Tests zu Sicherheitsbedrohungen haben kann (z. B. Nachschulung, aber keine personellen Konsequenzen; Vorgehen bei mehrmaligem Fehlverhalten innerhalb kurzer Zeit ist mit dem BR abzustimmen etc.)
- Arbeitnehmer:innen, die Opfer von Cyberattacken werden, erhalten größtmögliche **Anonymität**, um ihre Menschenwürde zu wahren
- Welche Aktivitätsprotokolle wie lange **aufbewahrt** werden
- Biometrische Merkmale sollten nur von einem eng begrenzten Personenkreis genutzt werden (z. B. jene mit Zugang zu streng vertraulichen Daten, Geschäftsgeheimnissen).

SKRIPTEN ÜBERSICHT



WIRTSCHAFT	
WI-1	Einführung in die Volkswirtschaftslehre und Wirtschaftswissenschaften
WI-2	Konjunktur
WI-3	Wachstum
WI-4	Einführung in die Betriebswirtschaftslehre
WI-5	Beschäftigung und Arbeitsmarkt
WI-6	Lohnpolitik und Einkommensverteilung
WI-9	Investition
WI-10	Internationaler Handel und Handelspolitik
WI-12	Steuerpolitik
WI-13	Bilanzanalyse
WI-14	Der Jahresabschluss
WI-16	Standort-, Technologie- und Industriepolitik
Die einzelnen Skripten werden laufend aktualisiert.	

POLITIK UND ZEITGESCHICHTE	
PZG-1A	Sozialdemokratie und andere politische Strömungen der ArbeiterInnenbewegung bis 1945
PZG-1B	Sozialdemokratie seit 1945
PZG-2	Christliche Soziallehre
PZG-4	Liberalismus/Neoliberalismus
PZG-6	Rechtsextremismus
PZG-7	Faschismus
PZG-8	Staat und Verfassung
PZG-9	Finanzmärkte
PZG-10	Politik, Ökonomie, Recht und Gewerkschaften
PZG-11	Gesellschaft, Staat und Verfassung im neuzeitlichen Europa, insbesondere am Beispiel Englands
PZG-12	Wege in den großen Krieg
PZG-14	Die Geschichte der Mitbestimmung in Österreich

SOZIALE KOMPETENZ	
SK-1	Grundlagen der Kommunikation
SK-2	Frei reden
SK-3	NLP
SK-4	Konfliktmanagement
SK-5	Moderation
SK-6	Grundlagen der Beratung
SK-7	Teamarbeit
SK-8	Führen im Betriebsrat
SK-9	Verhandeln
SK-10	Politische Rhetorik

Die VÖGB-Skripten online lesen oder als Gewerkschaftsmitglied gratis bestellen:
www.voegb.at/skripten

6 Nachwort

MS 365 zieht schneller neue Anwendungen aus seinen Programmier-Werkstätten, als dieses Skriptum fertiggestellt werden kann. Es wird also – so die Prognose der Autorin – noch vor Erscheinen dieser Publikation Neuigkeiten in der wunderbaren schnelllebigen Welt von MS 365 geben, die sich hier nicht wiederfinden können.

Um bei diesen schnellen Umdrehungen dennoch nicht schwindlig zu werden, ist eine fundierte Mitwirkung des Betriebsrats essenziell. Es braucht Zeit, um sich das Wissen zur Welt von MS 365 anzueignen, die betriebsspezifischen Anwendungen zu überblicken und dazu Vorgehensweisen zu vereinbaren sowie Routine zu entwickeln. Dies wissend, kann sich ein Betriebsrat auf das Wesentliche konzentrieren: die Grundpfeiler für eine Betriebsvereinbarung zu setzen, in der Beschäftigte vor den Risiken von MS 365 geschützt sind.

Grundrechte sind schnell verloren und langsam wiederzubeschaffen. Der Betriebsrat kann mit einer Betriebsvereinbarung dem Verlust dieser Grundrechte vorbeugen. Dieses Skriptum soll dabei helfen, die beste zum Unternehmen passende Betriebsvereinbarung auszuhandeln und Beschäftigte zu schützen. Nehmen wir uns die Zeit, um die Beschäftigten vor – offener oder versteckter, absichtlicher oder unbeabsichtigter – Überwachung und Eingriffen in ihre Privatsphäre zu bewahren.

VÖGB/AK-SKRIPTEN

Die Skripten sind eine Alternative und Ergänzung zum VÖGB/AK-Bildungsangebot und werden von ExpertInnen verfasst, didaktisch aufbereitet und laufend aktualisiert.

UNSERE SKRIPTEN UMFASSEN FOLGENDE THEMEN:

- › Arbeitsrecht
- › Sozialrecht
- › Gewerkschaftskunde
- › Praktische Gewerkschaftsarbeit
- › Internationale Gewerkschaftsbewegung
- › Wirtschaft
- › Wirtschaft – Recht – Mitbestimmung
- › Politik und Zeitgeschehen
- › Soziale Kompetenz
- › Humanisierung – Technologie – Umwelt
- › Öffentlichkeitsarbeit

SIE SIND GEEIGNET FÜR:

- › Seminare
- › ReferentInnen
- › Alle, die an gewerkschaftlichen Themen interessiert sind.

Nähere Infos und
kostenlose Bestellung:
www.voegb.at/skripten
E-Mail: skripten@voegb.at
Adresse:
Johann-Böhm-Platz 1,
1020 Wien
Tel.: 01/534 44-39244

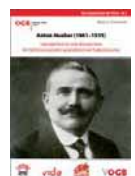


Die Skripten gibt es hier zum Download:



www.voegb.at/skripten

Leseempfehlung:
Reihe Zeitgeschichte und Politik



7 Anhang

Betriebsrät:innen, die in der Gewerkschaft GPA organisiert sind, erhalten von ihren Betriebsbetreuer:innen ein Muster, wie eine Basis-Betriebsvereinbarung zu MS 365 gestaltet werden kann.

Das „kleine Microsoft-Wörter-Buch“

API – eine Programmierschnittstelle, an der Anwendungen zusammenlaufen und Daten austauschen (Abk. für Application Programming Interface)

Backend – der für Nutzer:innen unsichtbare Teil von Anwendungen mit dem Programmcode, den Schnittstellen, der Verwaltung etc., wo in der Regel nur Administrator:innen Zugriff haben (deutsch: hinteres Ende, Unterbau)

Betriebssystem – das Hauptstück eines Computers, über das alle anderen Programme gestartet, gesteuert, verwaltet werden

Bing – Produktbezeichnung für die Suchmaschine von Microsoft (MS)

Browser – ein Programm zum Aufrufen von Internetseiten (deutsch: jemand, der/die durchstöbert)

Chatbot – ein Programm, das Sprache in Text umwandelt und Fragen scheinbar menschlich beantwortet (Kofferwort zusammengesetzt aus „Chat“ [deutsch: plaudern] und „Robot“)

ChatGPT – der erste Chatbot mit Künstlicher Intelligenz, der seit Ende 2022 weltweit gratis zur Verfügung steht (deutsch: Generative Pre-trained Transformer; generierender, vortrainierter Verwandler).

Copilot – Sammelbegriff von MS für Software, die mit Künstlicher Intelligenz arbeitet

Defender – Produktbezeichnung für ein Programm von MS, mit dem Geräte, Nutzer:innen und Netzwerke vor Sicherheitsgefahren geschützt werden (deutsch: jemand, der/die verteidigt)

Dienste – damit sind in der MS-Sprache nicht geheime Organisationen zum Schutz des Staates gemeint, sondern unterschiedliche Angebote, Produkte, Softwarepakete; meist dann, wenn sie online zur Verfügung gestellt werden

Edge – Produktbezeichnung für den Browser von MS (deutsch: Rand)

Explorer – Produktbezeichnung des früheren Browser von Microsoft (1995), wurde ersetzt durch Edge (deutsch: jemand der/die forscht)

Exchange – Produktbezeichnung für jenen Server von MS, auf dem E-Mails, Kalender, Kontakte und Aufgaben verwaltet, synchronisiert und für alle Geräte ausgetauscht werden (deutsch: Austausch)

Frontend – jener Teil eines Programms, auf den Nutzer:innen direkt Zugriff haben und wo sie durch eine Benutzeroberfläche ihre Aktionen durchführen können (deutsch: vorderes Ende, Vorbau)

Graph – Produktbezeichnung für jene zentrale Schnittstelle (=API) von MS, die alle anderen miteinander verknüpft

ID – eine Kennnummer, die jedem Gerät oder jedem/jeder Nutzer:in zugeordnet ist (engl. identity oder identification)

IP-Adresse – einmalige Kennnummer, die jedem Endgerät (Laptop, Handy etc.) zugeordnet ist und über die sich Geräte in einem Netzwerk erkennen und verbinden können

Meta – Big-Tech-Unternehmen, dem unter anderem Facebook, Instagram und WhatsApp gehören

Office – Produktbezeichnung für das Bürosoftwarepaket von MS, enthält die Software: Word, Excel, Powerpoint (deutsch: Büro, Amt, Geschäftsstelle)

Outlook – Produktbezeichnung von MS für Kalender, Kontakte und E-Mail (deutsch: Ausblick)

7 Anhang

Places – Produktbezeichnung von MS für eine Software, die den Standort des Geräts erfasst und damit Koordination der Büroflächen ermöglicht; ist mit Kalender eng verknüpft (deutsch: Plätze, Orte)

Purview – Produktbezeichnung für die Safety- und Security-Plattform von MS, wo Daten klassifiziert, ausgewertet und geschützt werden (deutsch: Zuständigkeitsbereich)

Rolle – in den Microsoft-Produkten ist den verschiedenen Nutzer:innen und Administrator:innen jeweils ein Zugriff zugeordnet

Sentinel – Produktbezeichnung für die Sicherheitsdaten aus der gesamten IT-Infrastruktur eines Unternehmens; arbeitet mitunter mit künstlicher Intelligenz und erkennt Angriffe in Echtzeit (deutsch: Wächter)

Server – ein starker Computer, auf dem die Software läuft und die Daten verarbeitet werden; es laufen immer mehrere in Netzwerken zusammen; in „Rechenzentren“ werden tausende davon übereinandergestapelt (deutsch: Zusteller, Servierer)

Skype – ein Programm, mit dem gratis mit Bild und Ton telefoniert wurde und erstmals auch größere Konferenzschaltungen möglich wurden; 2005 von e-Bay und 2011 von MS gekauft; 2025 wurde der Betrieb eingestellt (engl. Kofferwort mit „Himmel“)

Suchmaschine – eine Website, die nach Informationen im Internet sucht (dzt. meistverwendete ist Google)

Teams – Produktbezeichnung für eine Kommunikations- und Kollaborationsplattform von MS (deutsch: Gruppe, Mannschaft)

Tenant – jener Bereich auf Servern, der einem Unternehme oder einem Kunden (z.B. von MS) zugeordnet wird (deutsch: Mieter:in, Bewohner:in)

Viva – Produktbezeichnung für eine Plattform von MS, auf der verschiedenste Arbeitsmittel zur Verfügung gestellt werden (z.B. Lernmaterialien, persönliche

Zielsetzungen, Tipps zum Wohlbefinden etc.) und das Arbeitsverhalten ausgewertet wird

Website – alle Inhalte, Bilder, Texte etc., die zu einem Thema/einem Unternehmen im Internet angeboten werden; die Zusammenfassung mehrerer einzelner „Webpages“, einzelner Seiten

Windows – Produktbezeichnung für das Betriebssystem von MS (deutsch: Fenster)

Yammer – ehemalige Produktbezeichnung von MS für das soziale Netzwerk, das 2012 gekauft und 2023 eingestellt wurde (deutsch: quatschen, jammern)

8 Endnoten

- ¹ <https://www.heise.de/hintergrund/Microsoft-Abhaengigkeit-Bund-zahlt-in-einem-Jahr-fast-500-Millionen-Euro-11170931.html>; (abgerufen am 26.6.2026).
- ² <https://www.derstandard.at/story/2000122163418/microsoft-schafft-nach-kritik-office-365produktivitaetsbewertung-fuer-office-365-ab>; (abgerufen am 26.6.2026).
- ³ MS verspricht von Viva Glint: „Organisationen erhalten *sofortige Einblicke* in die Mitarbeitererfahrung mit organisationsweiten Umfragen und *empfohlenen Maßnahmen*, um Geschäftsergebnisse zu steigern. Fragen und Aktionspläne basieren auf der Personalwissenschaft, um *mitarbeiterbezogene Hör- und Engagementprogramme* zu unterstützen, die die Mitarbeitererfahrung unterstützen. Führungskräfte und Manager können Ergebnisse anzeigen, um Erfolge und Chancen zu verstehen, die *Leistung mit Benchmarks zu vergleichen* und personalisierte Vorschläge für Lernkurse, *Gesprächsstarter und andere Aktionen* zu erhalten, die positive Geschäftsergebnisse unterstützen.“ (Hervorhebung der Autorin) <https://learn.microsoft.com/de-de/office365/servicedescriptions/microsoft-viva-service-description>; (abgerufen am 26.6.2026).
- ⁴ Kritikpunkte außerhalb des Beschäftigtendatenschutzes finden sich auf Wikipedia <https://de.wikipedia.org/wiki/Microsoft#Kritik>.
- ⁵ OGH 14.07.2022 9 ObA 60/22x.
- ⁶ https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_de; (abgerufen am 26.06.2026).
- ⁷ <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>; (abgerufen am 26.06.2026).
- ⁸ Schrems vs Facebook Ireland I II und III C-311/18.
- ⁹ https://ec.europa.eu/commission/presscorner/detail/it/qanda_22_7632; (abgerufen am 26.06.2026).
- ¹⁰ Der Europäische Gerichtshof hat im Dezember 2024 festgestellt, dass eine solche Betriebsvereinbarung sich an die Grundsätze der DSGVO halten muss. Sie darf „*nicht gegen den Inhalt und die Ziele der DSGVO verstoßen*“ (Rechtssache C 65/23).
- ¹¹ Eine Anfrage zum entsprechenden „Cloud-Act“ seitens der besorgten französischen Parlaments im Juni 2025 wurde von MS bestätigt. <https://b2b-cyber-security.de/en/Microsoft-Cloud-access-to-EU-data-by-US-authorities-possible/>; (abgerufen am 26.06.2026).
- ¹² <https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data>; (abgerufen am 26.06.2026).
- ¹³ <https://www.microsoft.com/en-us/corporate-responsibility/reports/government-requests/customer-data>; (abgerufen am 26.06.2026).
- ¹⁴ Kriterien für eine gute Evaluierung wurden in deinem gemeinsamen Dokument von Arbeitsinspektion, Arbeiterkammer, Österreichischem Gewerkschaftsbund, Wirtschaftskammer und anderen in einer Broschüre zusammengefasst. https://www.arbeitsinspektion.gv.at/Zentrale_Dokumente/Uebergreifende_Themen/kriterieneineigutenevaluierungsbroschuere.pdf; (abgerufen am 26.06.2026).
- ¹⁵ <https://www.bloomberg.com/news/articles/2026-05-13/microsoft-spent-over-100-billion-on-openai-partnership-to-date>; (abgerufen am 26.06.2026).
- ¹⁶ <https://www.handelsblatt.com/technik/ki/ki-openai-stellt-sich-neu-auf-microsoft-bleibt-groesster-anteilseigner/100169025.html>; (abgerufen am 26.06.2026).
- ¹⁷ <https://www.golem.de/news/kuenstliche-intelligenz-openai-begrenzt-umsatzbeteiligung-fuer-microsoft-2604-208065.html>; (abgerufen am 26.06.2026).
- ¹⁸ <https://teybannerman.com/strategy/2026/03/31/how-many-microsoft-copilot-are-there.html>; (abgerufen am 26.06.2026).
- ¹⁹ Deloitte Australien wurde dabei „erwischt“ <https://orf.at/stories/3407637/>; (abgerufen am 26.06.2026).

Zur Autorin

Mag.^a Clara Fritsch ist Soziologin und Politikwissenschaftlerin. Sie arbeitet bei der Gewerkschaft GPA als Datenschutzexpertin, wo sie Betriebsratsgremien berät und trainiert, Betriebsvereinbarungen begutachtet und zum Thema publiziert.

