
# DIE WUNDERBARE WELT VON MICROSOFT

## und wie der Betriebsrat sie mitgestalten kann

Gewerkschaft GPA – Grundlagen, Arbeit und Technik

gpa MEINE GEWERKSCHAFT

**„Ein Agent geht über die Fähigkeiten einer generativen KI hinaus: Er assistiert nicht nur, sondern kann aktiv mit Ihnen zusammenarbeiten oder sogar eigenständig in Ihrem Namen handeln. (...) Das hilft Unternehmen dabei, Zeit und Geld zu sparen.“**

*(Microsoft, Zugriff am 14.1.2025)*

**„Alles ist mit allem verbunden.“**

*(eine Seminarteilnehmerin, November 2024)*

**„Es muss nicht immer Microsoft sein.“**

*(ein IT-Administrator, Dezember 2024)*

**IMPRESSUM:**
**Herausgeber:** Gewerkschaft GPA, 1030 Wien, Alfred-Dallinger-Platz 1
**Inhalt und Redaktion:** Clara Fritsch, Gewerkschaft GPA – Grundlagen, Arbeit & Technik
**Mitarbeit:** Andrea Kaindl, Gewerkschaft GPA – Grundlagen, Arbeit und Technik sowie Interessengemeinschaft IT
**Layout:** Christina Schier, Gewerkschaft GPA – Abteilung Organisierung und Marketing
**Bilder/Fotos:** iStock, Edgar Ketzer
ÖGB ZVR-Nr.: 576439352

Stand: Mai 2025

# AUTORIN

© Edgar Ketzer

**Mag.ª Clara Fritsch**

hat Soziologie und Politikwissenschaft studiert und arbeitet in der Abteilung Grundlagen, Arbeit und Technik der Gewerkschaft GPA. Arbeitsschwerpunkte sind Kontrolle am Arbeitsplatz, Beschäftigtendatenschutz, Microsoft, Personalentwicklungssysteme, Whistleblowing sowie algorithmische Entscheidungsfindung. Sie hält Seminare, Vorträge, berät Betriebsrätinnen und Betriebsräte und begutachtet Betriebsvereinbarungen.

# VORWORT

In den vergangenen Monaten machte Microsoft immer wieder Schlagzeilen. Es waren nicht gerade Erfolgsmeldungen, die wir da hören konnten. Im April 2024 kamen dem Tech-Konzern Microsoft beispielsweise Zugangsschlüssel zur zentralen Plattform (Master-Keys der Azure-Cloud) abhanden. Das Tech-Newsportal Heise nannte es den „Diebstahl der kryptographischen Kronjuwelen". Im Juli 2024 machte das für die Security bei Microsoft 356 zuständige Unternehmen Crowdstrike ein Update. Danach waren die Bildschirme in einigen infrastrukturell wichtigen Einrichtungen, wie Flughäfen oder Spitäler, schwarz. Im Juni 2024 rief Microsoft eine seiner neuesten Entwicklungen für das Betriebssystem Windows 11 zunächst zurück: die im Minutenabstand sämtliche Bildschirme unbemerkt und ungefragt fotografierende Erinnerungs- und Suchhilfe „Recall". Trotz massiver Bedenken ist „Recall" allerdings seit Herbst 2024 nun doch in Betrieb. Bis in die 2020er Jahre war es um den Tech-Konzern Microsoft verglichen mit Mitbewerbern wie Meta oder Alphabet medial eher ruhig. Mittlerweile macht das mit der Herstellung und dem Vertrieb von Betriebssystemen in den 1980er Jahren groß gewordene Unternehmen viel von sich reden. In diesem Geschehen lassen sich einige typische Eigenschaften von Microsoft erkennen.

Erstens: Das Angebot von Microsoft (MS) ist sehr breit aufgestellt. Neben der bekannten Bürosoftware „Office" und dem Betriebssystem „Windows" bietet Microsoft einiges mehr, wie zum Beispiel die Sicherheits- oder Überwachungssoftware „Purview" und „Sentinel", eine Suchmaschine namens „Bing", einen Browser namens „Edge", diverse Kommunikationssystemen wie „Teams" oder „Outlook", die mit künstlicher Intelligenz arbeitende Unterstützung „Copilot". Alles zusammen läuft in der Anwendung „Microsoft 365" auf Servern von Microsoft, also „in der Cloud".

# VORWORT

Zweitens: Microsoft ist schnell. Laufend werden Produkte neu erfunden, geändert, ergänzt, umbenannt und Funktionen anders zugeordnet. MS reagiert äußerst rasch und flexibel, sowohl in technischer als auch juristischer Hinsicht. Ein Beispiel dafür ist die Trennung von Teams und Microsoft 365 im April 2024, nachdem die EU-Kommission ein Verfahren wegen Verletzung des Wettbewerbsrechts eingeleitet hatte.

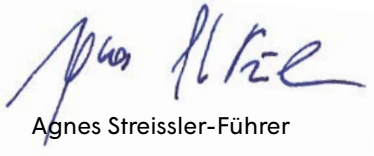
Und nicht zuletzt ist Software von Microsoft von unseren Arbeitsplätzen nicht mehr wegzudenken. Die Menschen sind den Umgang mit den verschiedenen Angeboten gewohnt. Ob privat oder im Betrieb, im Büro oder in der Fabrik, Microsoft bewältigt immer mehr Aufgaben des Arbeitslebens und ist immer weiter verbreitet.

Damit wird eine Vielzahl von Fragen aufgeworfen: Wer kann die Produktpalette noch überblicken? Wer hat das notwendige Knowhow, um die unzähligen Angebote, Einstellungen und Verbindungen in den verschiedenen Lizenzmodellen von MS 365 kritisch zu begutachten? Wie ist was womit und zu welchem Zweck verknüpft? Warum ändert sich ständig etwas bei Microsoft 365? Braucht es ein eigenes Wörterbuch, um MS 365 zu verstehen? Warum sollte man sich damit ausführlich beschäftigen? Und was geht das die Gewerkschaft an?

In dieser Broschüre wird den Fragen nachgegangen. Es braucht offensichtlich Hilfestellung für eine effektive Interessenvertretung bei der betrieblichen Verwendung von Microsoft-Produkten. Die Gewerkschaft GPA hat das vorliegende Werk in Angriff genommen, wissend, dass es nie vollständig, geschweige denn abgeschlossen sein wird. Wir wollen einen Überblick und Ansatzpunkte für den Umgang mit MS 365 bieten sowie Regelungen für Betriebsvereinbarungen aufzeigen.

Diese Broschüre zum betrieblichen Einsatz von Microsoft 365 spiegelt mit ihren vielen Querverweisen und den miteinander verzahnten Kapiteln die Welt von MS 365 wider. Die ersten Kapitel geben einen Ein- und **Überblick** zu MS 365. Danach beschäftigt sich die Broschüre mit den **arbeits- und datenschutzrechtlichen Aspekten** von MS 365. Die nach der Beratungserfahrung in der Gewerkschaft GPA am meisten eingesetzten sowie die heikelsten **Anwendungen von MS 365** werden im zweiten Teil skizziert. Im Abschluss werden die wichtigsten in einer **Betriebsvereinbarung** zu regelnden Punkte zusammengefasst. Die grauen Kästchen enthalten – je nach Symbol – Tipps zur Verwendung von MS 365 (durch Symbole mit Pfeilchen und Diamanten gekennzeichnet) beziehungsweise Zitate aus Betriebsvereinbarungen (Symbol mit Anführungszeichen). Auf diese Weise, sowie mit den Checklisten zum Schluss, wollen wir die Betriebsrätinnen und Betriebsräte dabei unterstützen, sich über die Software von MS 365 zu informieren und eine Betriebsvereinbarung dazu abzuschließen.

Viel Spaß beim Schmökern und viel Erfolg beim Umsetzen in Betriebsvereinbarungen.



Agnes Streissler-Führer

# INHALT

**Die Welt von Microsoft – was ist das Besondere an MS 365? . . . . . 8**
Interpretation von Beschäftigtendaten – was macht MS 365 mit unseren Daten? . . . . . 11

**Handlungsmöglichkeiten des Betriebsrates . . . . . 14**
MS 365 und die Arbeitsverfassung. . . . . 14
MS 365 und der Datenschutz. . . . . 16
MS 365 und der Gesundheitsschutz. . . . . 22

**Gestaltung der Basis einer Betriebsvereinbarung – wie MS 365 regeln?. . . . . 26**
Der Verwendungszweck. . . . . 28
Die Zugriffsbeschränkung. . . . . 29
Die Speicherdauer . . . . . 30
Die Privatnutzung . . . . . 30
Die Profile . . . . . 30
Die Kontrollmaßnahmen . . . . . 31
Die Schulung. . . . . 32
Die Einführung und die Aktualisierung. . . . . 33
Die Ansprechpartner:innen. . . . . 34

**Anwendungen für Nutzer:innen . . . . . 38**
Word, Excel, Powerpoint . . . . . 40
Outlook (= E-Mail, Kalender, Kontakt) . . . . . 41
Teams . . . . . 43
Status . . . . . 51
Viva . . . . . 52
ToDo . . . . . 55
Stream . . . . . 56
Planner. . . . . 56
Bookings . . . . . 57
Dynamics. . . . . 57
Forms . . . . . 58
Onedrive . . . . . 60

# INHALT


Visio . . . . . 61
Delve . . . . . 61
Skype . . . . . 62
Sprachassistenz . . . . . 62
Sway . . . . . 62
Bing . . . . . 62
Copilot . . . . . 62

**Anwendungen für Admins . . . . . 66**
Azure . . . . . 67
SharePoint . . . . . 67
Graph . . . . . 69
Power Platform, Power Automate & Fabrics . . . . . 70
AI Builder . . . . . 71
Exchange . . . . . 73
Purview und Purview Defender . . . . . 74
E-Discovery . . . . . 76
Compliance Portal . . . . . 77
Entra ID . . . . . 78
Entra ID Protection . . . . . 79
Data Loss Prevention . . . . . 79
Intune . . . . . 80
Sentinel . . . . . 81

**Arbeitsmaterial . . . . . 83**
Open-Source Alternativen zu Microsoft 365 . . . . . 83
Checkliste: (Basis-) Betriebsvereinbarung zu MS 365 . . . . . 86
Checkliste: MS 365 im Einklang mit DSGVO? . . . . . 87


 Besonderheiten in der Welt von MS 365

 Zitate aus bestehenden Betriebsvereinbarungen

 praktische Tipps

# DIE WELT VON MICROSOFT

## WAS IST DAS BESONDERE AN MS 365?

Der Konzern Microsoft (MS) ist bekannt für das weltweit meistgenutzte Betriebssystem „Windows". Das Unternehmen dürfte außerdem Marktführer bei Büro-Software sein – genaue Verkaufszahlen gibt es nicht. Microsoft hat in den letzten Jahren einen gewissen Monopolstatus erreicht. Microsoft-Produkte sind stark nachgefragt, nicht zuletzt, weil sie günstig und einfach verfügbar sind.

MS 365 (ehemals „Office 365") ist seit Oktober 2010 auf dem Markt und umfasst ein ausgesprochen **breites Angebot**. MS 365 enthält eine Menge einzelner Anwendungen (z. B. zur Kommunikation, Kollaboration, Sicherheit, Projektplanung, Mobile-Device-Management, Personalmanagement u.v.m.). Die meisten Ressourcen steckt Microsoft derzeit in den Ausbau der Anwendungen von Power Platform, das sind Anwendungen, die zum betriebsinternen Bedarf von den Kund:innen selbst programmiert werden [S. 70]. Auch in die verschiedenen Anwendungen von Viva fließt derzeit einiges Knowhow. Viva sind unterschiedliche Apps, die Nutzer:innen Verhaltensanalysen anbieten [S. 52]. Die meisten Kapazitäten nimmt momentan wohl die Implementierung von „Künstlicher Intelligenz" in diverse bereits vorhandene Produkte in Anspruch.

MS 365 hat auf **allen Organisationsebenen** etwas zu bieten. Sowohl für die einzelnen Beschäftigten auf individueller Ebene als auch für die Leitung (z. B. von Gruppen, Abteilungen und Bereichen) auf mittlerer Ebene, als auch für das Management auf höchster Ebene sind Anwendungen vorhanden. Es gibt Software, die für ein gesamtes Unternehmen von Bedeutung ist (z. B. die Plattform Sharepoint, die „Steuerungszentrale" Entra ID [S. 67] oder der „Türsteher" Defender [S. 74] etc.). Für das Management auf der Ebene von Gruppen, Bereichen, Abteilungen oder Niederlassungen hat MS 365 auch einiges im Angebot (z. B. die Plattform Teams [S. 43] oder die mit MS 365 verknüpfbare Plattform zur Personalverwaltung Dynamics [S. 57]) und für die einzelnen Nutzer:innen gibt es jede Menge Apps, sowohl zur Koordination mit anderen (z. B. Planner [S. 56], Outlook [S. 41]) als auch zur Organisation der persönlichen Arbeit (z. B. OneDrive [S. 60]).

Ein wesentliches Merkmal von MS 365 ist, dass diese Ebenen und Anwendungen alle über den sogenannten „Graph" [S. 69] miteinander verbunden sind. Wäre MS 365 ein lebender Organismus, wäre Graph das Herz.

Die einzelnen Anwendungen werden **permanent** ausgebaut, adaptiert, untereinander kombiniert, sprich: **verändert** oder „mit Erfahrungen angereichert" wie MS es ausdrückt. Anwendungen werden neu erfunden und in die bestehenden Apps integriert (z. B. wurde im Jänner 2022 Viva [S. 52] hinzugefügt). Manche Funktionen tauchen unter anderen Namen wieder auf (z. B. die Auswertungsmöglichkeiten von „Workplace Analytics" in „Viva Insights"). Anwendungen werden mit anderen zusammengespielt oder nicht mehr weiterentwickelt und „versickern" (z. B. wird Skype seit 2021 nicht mehr serviciert). So wurde die „Künstliche Intelligenz" zur **Emotionserkennung** auf Fotos im Juni 2022 wieder eingestellt – für ausgewählte Kundinnen und



Kunden steht ein Ableger davon allerdings weiter zur Verfügung, nämlich „Seeing AI“ für Blinde und Sehbeeinträchtigte. Immer wieder werden Apps, also Programme, von MS 365 umbenannt (z. B. wurden einige der Security-Apps unter dem Namen „Entra“ zusammengefasst). Es gibt also ununterbrochen Veränderungen in der Welt von MS 365.

MS enthält zusätzlich Funktionen, die quer über verschiedene Anwendungen aktiv sind (z. B. Standort, Präsenzstatus, Sprachsteuerung). Man könnte sie als **„Meta-Anwendungen“** bezeichnen. Beispielsweise kann die Spracherkennung in einem Word-Dokument im Sinne eines Diktiergeräts zum Einsatz kommen sie kann für das Transkribieren von Chats in Teams verwendet werden oder auch zum Erteilen von Befehlen zum Vorlesen von E-Mails und Kalendereinträgen.

MS kauft andere Unternehmen und integriert deren wesentliche Anwendungen in die eigene Produktpalette.

- 2011 **Skype**, um die **Videotelefonie** verstärkt einzubinden;
- 2013 die Handysparte von **Nokia**, um sie, nach wenig erfolgreichen Versuchen mit dem **Handy** Lumia und dem Betriebssystem Windows Phone, 2018 an Foxconn zu verkaufen (Der zweite Versuch mit einer eigenen Handymarke, Surface, wurde nach wenigen Jahren 2024 ebenfalls wieder eingestellt);
- 2016 wurde die **Plattform** für berufliche Vernetzung und Karriereförderung **LinkedIn** übernommen;
- 2018 wurde die **Programmierplattform GitHub** gekauft;
- 2022 die bisher teuerste Akquise von Microsoft um 75,4 Milliarden US Dollar, der Computerspielkonzern **Activision Blizzard**, womit mehr bewegte Bilder und aufwendigere Grafiken Einzug halten

MS 365 beinhaltet zusätzlich zu den eigenen, miteinander verflochtenen Anwendungen, Möglichkeiten zur **Einbindung externer** Apps/Software/Programmen/Anwendungen. Es können beliebige Erweiterungen eingebunden werden (beispielsweise aus anderen Welten, wie Cisco Webex oder Zoom).

Seit dem Erwerb der Plattform LinkedIn durch MS ist eine zusätzliche Schaltfläche im Mailprogramm Outlook vorhanden. Dadurch werden die Konten auf Outlook und LinkedIn miteinander abgeglichen. Was auf LinkedIn steht, ist auch auf Outlook sichtbar  Abb. unten).

Dass die Verbindung zwischen LinkedIn und Microsoft voreingestellt ist, kann bei Nutzer:innen Unbehagen auslösen. Die Verbindung ist jedoch nicht für die Ewigkeit; sie lässt sich lösen.

Über die Gruppen-Richtlinien im Entra Admincenter [S. 57] kann die Verbindung zwischen LinkedIn und dem Microsoft-Konto getrennt werden. Voraussetzung dafür ist eine Entra-Administrator- oder Global-Admin-Rolle im Lizenzmodell E3 oder E5.

Die Zukäufe und Erweiterungen machen den Umgang mit MS 365 nicht übersichtlicher.

Eines ist sicher: **MS 365 ist immer in Bewegung**.

MS 365 kann auf unterschiedliche Art betrieben werden. MS 365 kann auf firmeneigenen Servern laufen (die Bezeichnung dafür lautet „on premise“) oder die Apps werden aus der **Cloud** heruntergeladen und / oder dort betrieben. MS 365 kann weitgehend verwendet werden, ohne dass firmenintern Systemadministrator:innen tätig werden oder firmeneigene Server erforderlich sind.

Bei dieser Cloud-Variante von MS 365 findet die Datenverarbeitung auf Servern von MS statt, wobei die Kund:innen/Nutzer:innen/Unternehmen nur auf ihre eigenen Datenbestände Zugriff haben (sollten).

Die MS Server sind verstreut über **unterschiedliche Standorte**. In Europa liegen die großen Serverfarmen für die Cloudanwendungen derzeit in Amsterdam, Dublin, Frankfurt, Berlin, Magdeburg, Mailand, Zürich, Genf, London, Cardiff, Madrid, Oslo, Stravanger, Warschau, Budapest und Bukarest. In Wien Gerasdorf ist gerade eines in Bau. Jedes der Rechenzentren hat einen „Zwilling“, um bei Ausfällen sofort ausweichen zu können und so die Kapazitäten zu erhalten.

Um den **Energiebedarf** von MS Dienstleistungen, der nicht zuletzt durch KI entsteht, decken zu können, ist ein Ausbau der Rechenzentren unumgänglich. In Pennsylvania, USA, plant MS daher 2028 ein stillgelegtes Atomkraftwerk wieder in Betrieb zu nehmen.

Es ist nicht immer möglich, den tatsächlichen Speicherort ausfindig zu machen. Wenn Daten durch die Nutzer:innen selbständig verschlüsselt werden, kann es sein, dass auch MS nicht mehr feststellen kann, auf welchen Servern die Daten physisch liegen. Die in der Europäischen Datenschutzgrundverordnung (DSGVO) verankerten Grundsätze der Transparenz und Rechenschaft sind mit  unbekannten und mitunter außerhalb der EU liegenden Speicherorten nicht vereinbar. Um der Kritik entgegenzuwirken, beteuert MS im Mai 2021 „alle zentralen Cloud-Dienste von Microsoft – Azure, Microsoft 365 und Dynamics 365“ auf Europäischen Serverfarmen zu speichern und bietet „hochwirksame Verschlüsselungen und robuste Lockbox-Lösungen“.

**DIE VERBINDUNG VON MS 365 MIT LINKEDIN: INFORMATIONEN AUCH OHNE ZUSTIMMUNG**

ⓘ Wichtig

Die LinkedIn-Integration ist zwar erst vollständig aktiviert, wenn Ihre Benutzer der Verbindung mit ihren Konten zustimmen, aber der Zugriff auf öffentliche LinkedIn-Profilinformationen ist verfügbar, ohne dass eine individuelle Zustimmung erforderlich ist. Die vollständige Integration (bidirektionale Zustimmung und zusätzliche Felder) ist ohne Zustimmung jedes Benutzers nicht aktiviert. Ihre Benutzer können das verfügbare LinkedIn-Profil jeder Person sehen, die dem gesuchten Namen entspricht, unabhängig davon, ob sich diese Übereinstimmung in derselben aktivierten Gruppe befindet oder nicht.

Bei MS Cloud-Anwendungen wird die Software nicht auf unternehmenseigenen Servern installiert, gewartet, aktualisiert, repariert, ausgetauscht, ergänzt etc. Für die meisten Unternehmen liegt darin ein Vorteil, da zeit- und ressourcenintensive Aufgaben wegfallen. Personal, Speicher- und Rechnerkapazitäten, IT-Know-how, Bug-Fixes (also das Beheben von Software-Fehlern), Updates (also Aktualisierungen und Erweiterungen der Software), das alles stellt MS zur Verfügung – und muss dazu nicht das Firmengelände betreten. IT-Verantwortliche berichten allerdings aus der Praxis, dass ihre Kapazitäten dennoch gefragt sind, da das betriebsspezifische Einrichten, das Erstellen der Richtlinien, das Verfolgen der permanenten Updates einen zumindest ebenso großen Aufwand darstellen, wie die IT-Arbeit vor dem Umstieg auf Microsoft (Alternativen sind im Anhang aufgezeigt [S. 83]).

Die **Verfügbarkeit und Stabilität** dürften bei MS 365 verlässlicher sein als bei den meisten firmenintern betriebenen Systemen. Sollten MS Anwendungen versagen, hat das jedoch gravierende Auswirkungen, wie im Juli 2024 der Update-Fehler des bei MS 365 für die Security zuständigen Betreibers Crowdstrike. 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, riesig aufgrund der weiten Verbreitung von MS.

Werden Anwendungen von MS genutzt, hat das den Nebeneffekt, dass sämtliche Nutzungsdaten (auch Metadaten oder Telemetriedaten genannt, zu deren Interpretation siehe [S. 40] bei MS landen. MS kann damit Vergleiche anstellen, Schwellenwerte erzeugen ab denen etwas als „gut" oder „schlecht" bewertet wird (englisch: „Benchmarks"), Rückmeldungen einholen, Anwendungen „verbessern" und den Bedarf an neuen Anwendungen analysieren. Dieser Datenschatz und die darauf basierenden Innovationen sind es, die MS groß gemacht haben.

**Die Vorteile liegen auf der Hand.**

- MS funktioniert weitgehend stabil, weil sich die über den gesamten Erdball verteilten Serverfarmen bei Problemen gegenseitig ersetzen.
- MS bietet orts- und zeitunabhängiges Arbeiten, weil die Server rund um die Uhr und von jedem Standort aus erreichbar sind und permanent gewartet (engl. „serviciert") werden.
- Kontinuierliche Zahlungen in Form von Lizenzgebühren sind für Unternehmen besser planbar.
- MS Produkte sind auf dem letzten Stand der Technik, weil permanent Updates durchgeführt werden.

## 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 [S. 69] verknüpft. Jede Anwendung kreiert im Hintergrund Verbindungs- und Verhaltensdaten (auch Metadaten oder Telemetriedaten genannt). Technisch ist das nicht anders möglich und es kann nicht berücksichtigt werden, ob Nutzer:innen das wollen oder nicht. Dabei handelt es sich nicht nur um die Nutzungsdaten Einzelner (z. B. deren individuelle Vorlieben bei Einstellungen, deren persönliche E-Mail-Regelungen, die Nutzungshäufigkeit, deren bevorzugte Nutzungszeiten etc.), sondern auch um die Beziehungen der einzelnen Nutzer:innen untereinander (z. B. durchschnittliche Reaktionsgeschwindigkeit zu verschiedenen Empfänger:innen, häufige Kommunikationspartner:innen, Vergleiche innerhalb einer Gruppe etc.). So kann nicht nur zu jedem Nutzer und jeder Nutzerin, sondern auch zu jeder Gruppe, jedem Team, jeder Abteilung ein vergleichendes Profil zusammengestellt werden.

In einigen Anwendungen wird der **Präsenzstatus** der Nutzer:innen angegeben (z. B. Outlook, Office, Teams) oder die Nutzung mit einem Zeitstempel versehen (z. B. wann wurde eine Datei bearbeitet, wann wurde ein Chat geschrieben, wann ist jemand einem Meeting beigetreten) und somit wird die Aktivität der Beschäftigten punktgenau nachvollziehbar beziehungsweise vergleichbar. Egal ob die Statusfunktion selbständig deaktiviert wurde oder nicht, laufen die Protokolle im Hintergrund jedenfalls mit und sind somit vorhanden.

Ist technisch eine Kontrolle der Arbeitnehmer:innen gegeben, muss versucht werden diese über technische oder organisatorische Maßnahmen einzuschränken. Die Interpretation dieser Daten darf nicht zu Lasten der Beschäftigten gehen. Idealerweise werden beispielsweise Statusinformationen nicht weiter interpretiert - außer als eine Auskunft darüber, ob MS erfasst, dass jemand gerade beschäftigt sei oder verfügbar.
MS 365 in der Cloud ist permanent online und übermittelt ununterbrochen Daten an Microsoft, unter anderem solche, die zur Stabilität und Sicherheit erforderlich sind. Der Verwendungszweck dieser Daten „zur Verbesserung der Produkte und Dienstleistungen" wie es bei MS lautet, kann und wird von MS umfassend interpretiert.

Beispiele für **Interpretationen**, die von MS-Anwender:innen festgestellt wurden und die durchaus kritisch zu sehen sind:

- haben Nutzer:innen Terminkollisionen in ihren Kalendern, geht man in der MS-Logik von „abgelenkten Teilnehmern" aus. Es könnte aber schlicht daran liegen, dass ein abgesagter Termin nicht gelöscht wurde.

- sind einem Termin keine weiteren Teilnehmer:innen zugeordnet, wird der Termin als mögliche „Fokuszeit" angezeigt. Fokuszeit wird den Nutzer:innen vorgeschlagen, um ungestört und konzentriert arbeiten zu können. Um die beste Fokuszeit herauszufiltern, wird ausgewertet, wie „aktiv" jemand ist. Dazu werden vermutlich Aktivitäten gemessen und mit der Verweildauer in einer App in Beziehung gesetzt. So schlägt MS z. B. Termine als potenzielle „Fokuszeiten" vor, bei denen es sich tatsächlich um ein Webinar mit Teilnehmenden außerhalb der über Outlook bekannten Kontakte handelt oder etwa einen Arzttermin.

- Bestehen viele Interaktionen mit Personen aus den MS-Kontakten (z. B. gemeinsame Termine, gemeinsam bearbeitete Projekte, geteilte One-Drive-Dokumente etc.), wird dieser Umstand positiv beurteilt. Kolleginnen oder Kollegen mit hohem „Vernetzungsgrad" werden von MS als „erfolgreich" bewertet – wer kein ausgedehntes Netzwerk hat, gilt als weniger erfolgreich. 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 ein verständliches.

- Mittels Power BI [S. 70] oder Viva Glint [S. 54] können Gruppen und Meetings analysiert werden. Ein „Owner", also Eigentümer, der oder die die Analyse startet, kann jederzeit die Beteiligung der Teilnehmer:innen auswerten (z. B. bei Aktivitäten auf der Plattform Teams: Pünktlichkeit, hochgeladenen Dateien, eingebrachte mündliche Statements...), ganz ohne Zustimmung des/der Einzelnen.

- „Viva Insight" [S. 52] berechnet, wann die individuell besten Zeitfenster für „well-being" (deutsch: Wohlbefinden) bestehen, wobei meist einfach freie Zeitfenster im Kalender angezeigt werden, genauere Berechnungsgrundlagen im Dunkeln bleiben.

- „Viva Insight" [S. 52] verrät Tipps wie „deaktivieren sie Arbeit außerhalb der Arbeitszeit". In der MS 365-Welt ist jedoch alles, was außerhalb der MS-Anwendungen geschieht, keine Arbeitszeit.

MS 365 kann nur jene (Verbindungs-)Daten verarbeiten, die mit MS-eigenen oder mit MS verknüpften Apps erstellt werden. MS geht davon aus, dass sämtliche Arbeitsaktivitäten innerhalb der Welt von MS ablaufen. Arbeitet jemand mit einer Suchmaschine außerhalb des MS-Universums (z. B. duckduckgo), schreibt Nachrichten auf einer MS-unabhängigen App (z. B. Signal), benutzt einen anderen Kalender als den von Outlook (z. B. google calendar), postet auf Social-Media (z. B. mastodon), leitet eine Videokonferenz, die nicht von MS stammt (z. B. Zoom), fließen diese Aktivitäten nicht in die Interpretationen von MS ein. Arbeitszeit, die nicht mit MS Anwendungen verbracht wird, wird von MS als „Inaktivität" oder Freizeit interpretiert. (Zu den Alternativen Anwendungen siehe Anhang [S. 83].)

MS 365 errechnet also Zusammenhänge, die nicht



unbedingt sinnvoll sind und trifft damit Aussagen über Sozialverhalten, zeiteffizientes Verhalten (siehe z. B. Viva S. 52), oder finanzielle Effekte (siehe z. B. Dynamics [S. 57]).

Nachdem die Rechenmodelle im Hintergrund aber nicht offengelegt werden, ist nicht ersichtlich, ob die Grundannahmen sinnvoll sind. Genauso unklar bleibt, ob ethische Grundprinzipien mit einfließen und rechtliche Vorgaben eingehalten werden (z. B., dass Entscheidungen aufgrund von maschinellen Berechnungen jederzeit widerrufbar sein müssen). 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 massig 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. In welchem Ausmaß 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 übermittelt an Microsoft Telemetriedaten über den Systemzustand und über Nutzer:innenaktivitäten. Dies kann technisch nicht ausgeschlossen werden. Es ist jedoch seitens der lokalen Systemadministrator:innen sicherzustellen, dass diese Daten nicht geeignet sind, Aussagen über identifizierbare Personen zu treffen, insbesondere, dass keine Benutzer-ID, Betreffzeilen oder Inhaltsdaten in den übermittelten Telemetriedaten enthalten sind.]

Admins können über sog. Gruppenrichtlinien einstellen ob und in welchem Umfang Diagnosedaten erfasst und an Microsoft übermittelt werden (z. B. über Lokale Firewall-Regeln, Deaktivierung der Telemetrie gemäß Microsoft z. B. auf Windows Server, Enterprise oder Education oder Deaktivierung von Telemetrie Dienst und dazugehörigen „Event Tracing for Windows Autologger".)

# HANDLUNGS-MÖGLICHKEITEN DES BETRIEBSRATES

Aus dem **Arbeitsverfassungsgesetz (ArbVG)**, dem Arbeitnehmer:innenschutzgesetz (ASchG) und der Europäischen Datenschutzgrundverordnung (DSGVO) ergeben sich Möglichkeiten, wie sich Betriebsrät:innen bei der Gestaltung von MS 365 einbringen können.

- Betriebsrätinnen oder Betriebsräte können sich darauf berufen, dass sie die Einhaltung von **gesetzlichen Vorgaben überwachen** müssen (z. B. wenn sie Einsicht in Auswertungen nehmen wollen). Um den Kontrollpflichten nachkommen zu können, hat der Betriebsrat oder die Betriebsrätin (BR) verschiedene Möglichkeiten. Beispielsweise kann sie oder er eine eigene „Rolle", eine Leseberechtigung, für MS 365 einfordern [S. 29]. Der BR kann eine MS 365-Datenschutzgruppe mit regelmäßigen Informationstreffen ins Leben rufen [S. 35]. Der BR kann fixe Abläufe zur Informationsweitergabe einfordern, die bei Änderungen von MS 365 einzuhalten sind.

- Sie oder er kann eine **Anhörung** verlangen, bei der von Seiten des Betriebsrats **Vorschläge** zur Gestaltung oder Deaktivierung von einzelnen Anwendungen vorgebracht werden.

- Sie oder er kann eine umfassende **Information** verlangen (z. B. welche Anwendungen in Betrieb sind, wer Einsichtsrechte hat, welche Daten miteinander verknüpft werden, wo Daten gespeichert werden etc.). Hilfestellung dazu geben die zwei Checklisten im Anhang [S. 86 sowie Beiheft].

- Sie oder er kann Schulungen und Qualifizierungen für die Beschäftigten verlangen oder auf eine **Unterweisung** bestehen, wie die „Betriebsmittel" – denn im Grunde ist die Software von MS nichts anderes – verwendet werden müssen (siehe §§ 12–14 ASchG).

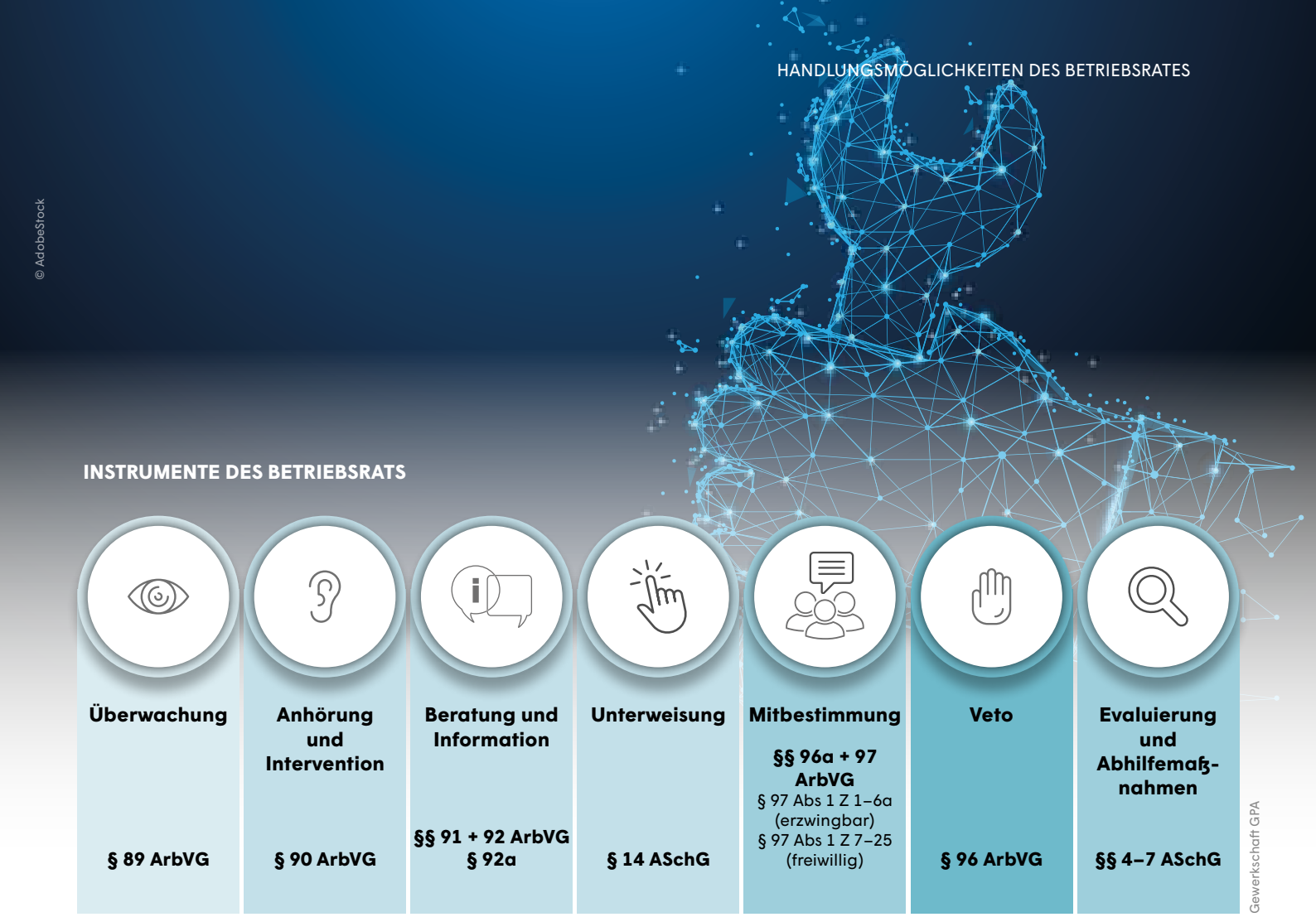
- Sie oder er kann und soll **Einsicht** verlangen in die Ergebnisse der **Evaluierung** und der **Abhilfemaßnahmen** gegen gesundheitliche Gefahren (z. B. psychische Belastung durch steigende Kontrollmöglichkeiten, Stress durch Überzahl an Kommunikationskanälen, Überforderung durch mangelndes Wissen; siehe §§ 4 und 5 ASchG sowie [S. 21–23].

- Der Betriebsrat hat das Recht eine **Betriebsvereinbarung** durchzusetzen.

Es stehen dem Betriebsrat also einige rechtliche Bestimmungen zur Verfügung, mit denen die Interessen der Belegschaft vertreten und durchgesetzt werden können (siehe Abbildung „die Instrumente des Betriebsrats").

### MS 365 UND DIE ARBEITSVERFASSUNG

Das österreichische Arbeitsverfassungsgesetz sieht in diversen Fällen die Mitwirkung des Betriebsrats vor. Die wichtigste Bestimmung in Zusammenhang mit technischen Kontrollsystemen, und als solches kann MS 365 bezeichnet werden, gibt vor, dass „die Einfüh-




rung 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"**. Aufgrund dieser Bestimmung ist also zu (fast) jeder Art von Software von MS 365 eine Betriebsvereinbarung erforderlich, denn (fast) jede Software von MS 365 ist dazu geeignet, Arbeitnehmer:innen zu kontrollieren. Angesichts der lückenlosen Aufzeichnung des Nutzungsverhaltens, ist anzunehmen, dass eine Betriebsvereinbarung gemäß § 96 Abs 1 Z 3 ArbVG abzuschließen ist.

Die juristischen Begriffe aus dem Arbeitsverfassungsgesetz (ArbVG) „Kontrollmaßnahme" bzw. „technische Systeme zur Kontrolle der Arbeitnehmer:innen" sind im weiten Sinne zu verstehen. Es kommt dabei nicht auf eine subjektive Absicht zur Überwachung durch den oder die Arbeitgeber:in an, sondern auf eine **objektive Eignung** der Maßnahme bzw. des Systems zur Kontrolle. Die bloße Möglichkeit zur Kontrolle reicht aus, damit ein System zustimmungspflichtig ist. Das Erfassen von Verbindungsdaten, Standortdaten, Präsenzstatusangaben, der zeitlichen Dauer von Interaktionen sind zahlreiche Möglichkeiten zur Kontrolle von Arbeitnehmer:innen. Diese umfangreichen Datensammlungen von MS 365 sind mit an Sicherheit grenzender Wahrscheinlichkeit allein schon durch ihre Vielzahl und ihr stetes Vorhandensein eine Kontrollmaßnahme. 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 Jurist:innen, wenn bei den überwachten Personen das Gefühl einer laufenden Überwachung entsteht, die Kontrolle also über das für die Arbeitserbringung unbedingt nötige Maß hinausgeht. Nachdem von MS 365 sehr viele Arbeitsprozesse erfasst sind oder zumindest sein können, kann eine lückenlose Aufzeichnung der Tätigkeiten von Arbeitnehmer:innen erfolgen.

Soll beurteilt werden, ob die Menschenwürde nun berührt ist, ob also eine Betriebsvereinbarungspflicht gegeben ist, muss beachtet werden, was **konkret im Betrieb im Einsatz** ist. Betriebsrät:innen, die eine Betriebsvereinbarung durchsetzen möchten, müssen nachweisen, wie die Kontrolle erfolgt. 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 Juli 2022, es müsse zuerst festgestellt werden, ob ein verwendetes System tatsächlich in der Lage ist, die Menschenwürde zu berühren, um eine Betriebsvereinbarungspflicht daraus abzuleiten.

Das ArbVG beinhaltet weitere Grundlagen für den Abschluss einer Betriebsvereinbarung: die „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), sowie die „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), bedürfen der Zustimmung des Betriebsrates. Stimmt der Betriebsrat der Verwendung eines solchen Systems nicht zu, kann die Zustimmung auf Grundlage des § 96a ArbVG durch eine Entscheidung der Schlichtungsstelle ersetzt werden (**„ersetzbare Zustimmung"**).

Obwohl das Gesetz von der „Einführung" bestimmter Maßnahmen oder Systeme spricht, bezieht es sich auch auf bereits bestehende Systeme. Erweiterung, Abänderung, Verknüpfung zweier Systeme oder auch die teilweise Rücknahme sind damit gleichfalls gemeint. Werden beim Einsatz von MS 365 also **substanzielle 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.

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

## MS 365 UND DER DATENSCHUTZ

Neben arbeitsverfassungsrechtlichen Aspekten spielt auch das Datenschutzrecht eine wesentliche Rolle beim Einsatz von MS 365. Das Bestehen einer Betriebsvereinbarung ändert nichts daran, dass die Bestimmungen der Europäischen Datenschutzgrundverordnung (DSGVO) und des österreichischen Datenschutzgesetzes (DSG) eingehalten werden müssen.

Gemäß gesetzlicher Definition gehören zu den „personenbezogenen Daten" nicht nur langläufig bekannte Angaben, wie Name, Geburtsdatum oder Anschrift, sondern auch IP-Adresse, Standort, Handy-Nummer, Zimmernummer, Personalnummer, Personenkennzeichen wie die Sozialversicherungsnummer oder das Nummernschild eines Autos; kurz alle Daten, die einer oder einem Beschäftigten zugeordnet werden können. 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 DSG), darunter insbesondere die **Rechte auf Auskunft, Berichtigung und Löschung** (Art. 15 ff DSGVO).

Betroffene, also auch Beschäftigte, die MS-Anwendungen nutzen (müssen) und deren personenbezogene Daten verarbeitet werden, haben Anspruch auf **Auskunft** 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. Der oder die Verantwortliche hat auf ein solches Auskunftsbegehren binnen vier Wochen Auskunft zu geben.
Bewahrt der oder die 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 auch dann, wenn Daten ohne Rechtsgrundlage erhoben wurden oder wenn der Verwendungszweck nicht mehr gegeben ist, wenn sie also nicht mehr gebraucht werden.

Ganz grundsätzlich dürfen Verantwortliche die personenbezogenen Daten der Beschäftigten nicht ewig aufbewahren. Stets müssen eine **Rechtsgrundlage** und ein konkreter (Verarbeitungs-)**Zweck** gegeben sein.

Liegt etwa 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.

Zugegeben, bei MS 365 ist es schwierig für den Verantwortlichen, also den oder die Arbeitgeber:in, alle diese Rechte zu erfüllen. Mitunter fehlt es schlicht an Wissen, welche Daten verwendet werden, ob an Dritte wie MS und dessen Subunternehmen weitergeleitet wird, oder wie lange aufbewahrt wird – mitunter trotzdem Daten bereits aus dem System gelöscht wurden. Dazu ist zu sagen, dass Arbeitgeber sich dennoch dieser Verantwortung stellen müssen. Sie müssen für die Verwendung in ihrem Unternehmen – und nicht für die Verwendung bei MS – die datenschutzrechtlichen Grundlagen erfüllen, also Auskunft erteilen, die Rechtsgrundlage anzuführen, den Verwendungszweck festlegen.

**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 (ebenso wie jeder andere Verarbeitungsvorgang) einer Rechtsgrundlage, in Zusammenhang mit der DSGVO spricht man von einem Auftragsdatenverarbeitungsvertrag (AVV). Dieser dient dazu, die Rechte und Freiheiten der Personen zu schützen und muss daher Art und Zweck, Speicherdauer, die Pflichten der verantwortlichen Person sowie des oder der Auftragsdatenverarbeiter:in beinhalten. Microsoft bietet einen solchen Standardvertrag an. Im September 2022 wurden diese AVV von Microsoft an die durch ein EuGH-Urteil entstandene Rechtslage1[1] angepasst und MS nennt sie nun „**Microsoft Products and Services Data Protection Addendum (DPA)**"[2]. Mittels dieser Verträge soll die Datenverwendung von personenbezogenen Daten bei MS in den USA legalisiert werden.

Dass MS Daten von EU-Bürger:innen in den USA verarbeitet war (und ist) problematisch. Im sogenannten Schrems-Urteil hat der EuGH (bereits mehrmals) festgestellt, dass der Schutz von Daten von EU-Bürger:innen in den USA nicht im selben Ausmaß gegeben ist, wie in Europa.

Am 4. Juni 2021 verabschiedete die Europäische Kommission daher zwei Sätze von **Standardvertragsklauseln** (SCCs), die die alten Klauseln ersetzen und die Übermittlung personenbezogener Daten zwischen der EU und Drittländern ohne Angemessenheitsbeschluss erleichtern sollen. Diese Standardvertragsklauseln wurden aufgrund eines EuGh-Urteils wieder zurückgenommen.

Am 10. Juli folgte ein neues Abkommen für den rechtmäßigen Datentransfer zwischen USA und EU; die „Adequacy decision for the **EU-US Data Privacy Framework**"(DPF).

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

Die meisten Server für europäische Microsoft-Kundinnen oder -Kunden stehen mittlerweile in Europa. Dennoch kann Microsoft nicht gänzlich ausschließen, dass personenbezogene Daten in den USA verarbeitet

1 https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_de (Letzter Zugriff: 19.12.2024)
2 https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA (Letzter Zugriff: 19.12.2024)

werden und somit nach US-amerikanischem Recht auch den dortigen Geheimdiensten zur Verfügung gestellt werden. Microsoft versucht zwar, eine solche Auslieferung zu unterbinden, doch gelingt das nicht immer (zur Strafverfolgung den USA siehe S.20).

**Datenschutzfolgenabschätzung (DSFA)**

Muss eine DSFA erstellt werden, sollte vorab in einer so genannten „**Schwellenwertanalyse**" eingeschätzt werden, welches Risiko für die Grundrechte der Nutzer:innen bei den verwendeten MS 365-Apps besteht. Der Betriebsrat ist bei der Datenschutzfolgenabschätzung einzubeziehen (Art. 35 DSGVO). „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 der oder die Arbeitgeber:in eine Datenschutzfolgenabschätzung durchführen. Im Zuge der DSFA muss auch dafür gesorgt werden, dass **Maßnahmen zum Schutz der Privatsphäre** getroffen werden. Dabei kann sich herausstellen, dass bestimmte Systemanpassungen zur Risikominimierung beitragen können. „Gibt es Einstellungen, die die Privatsphäre besser schützen würden?", lautet die maßgebliche Frage, um Abhilfemaßnahmen zu finden.
Die DSFA soll dazu dienen, bereits im Vorfeld einer Datenverarbeitung Risiken für die Betroffenen zu erkennen, Gegenmaßnahmen zu ergreifen und nicht zuletzt das durch Datenschutzverletzungen entstehende wirtschaftliche Risiko zu minimieren. Eine rückwirkende Regulierung ist im Datenschutz schwer möglich – passiert eine Rechtsverletzung, ist es bereits zu spät.

Bei der DSFA ist der oder die betriebliche Datenschutzbeauftragte beizuziehen. Zusätzlich sind die **Standpunkte der Betroffenen und ihrer Vertretung** anzuhören (Art. 35 Abs. 9 DSGVO). Dem Betriebsrat kommt im Rahmen der DSFA also eine wichtige Rolle zu. Die DSFA ist – neben dem Artikel 88 DSGVO – der einzige Ansatzpunkt in der DSGVO für explizit angesprochene Mitwirkungsrechte der betrieblichen Interessenvertretung, also des Betriebsrats. Rechtlich verantwortlich für die Durchführung der DSFA ist der oder die Arbeitgeber:in und nicht der Betriebsrat.

Gerade die systematischen Auswertungen 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. Sollten Anwendungen von MS 365 mit sogenannter „**Künstlicher Intelligenz**" (KI) zum Einsatz kommen, ist ebenso eine DSFA erforderlich. Künstliche Intelligenz bietet MS 365 unter anderem mit dem Copilot [S. 62] an, beispielsweise bei Authentifizierung über Sprache, bei der Textanalyse, die „Gefühle" erkennt oder bei der Verhaltensanalyse, die wahrscheinlich auftretenden Ereignisse personenbezogen prognostiziert. Die **EU-Verordnung zur Künstlichen Intelligenz** (EU AI Act) hält fest, dass: „(...) die Verwendung von KI-Systemen zur Ableitung von Emotionen einer natürlichen Person in den Bereichen Arbeitsplatz (...)" nicht erlaubt ist. (Art.5 (1) f) EU KI VO) MS investiert derzeit immens in den Ausbau von KI-Modellen, beispielsweise bei der Firma „OpenAI" und deren Produkt „ChatGPT" (siehe Copilot [S. 62].

Die Gewerkschaft GPA hat Tipps zusammengestellt, welche Prüfschritte und Fragestellungen für die DSFA und die Beteiligung des Betriebsrates relevant sind. Diese Unterlagen sind bei den betriebsbetreuenden Sekretären und Sekretärinnen der GPA erhältlich.

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...". ArbVG und DSGVO ergänzen einander.

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).



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

Immer wieder wird MS dafür kritisiert, sich nicht an die Europäische Rechtslage zum Datenschutz, die Datenschutzgrundverordnung (DSGVO), zu halten. Mehrere Umstände lassen tatsächlich daran zweifeln, dass MS 365 DSGVO-konform ist:

**Speicherfristen** können unternehmensspezifisch von der IT-Abteilung definiert und somit unmittelbar an den Zweck der Datenverarbeitung gebunden werden. Gemäß DSGVO dürfen personenbezogene Daten so lange aufbewahrt werden, als sie einem legitimen Zweck dienen.

**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.

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, Systeme „Künstlicher Intelligenz", die „selbst lernen", die personenbezogene Daten der Nutzer:innen verwenden (z. B. Viva [S. 52], Dynamics [S. 57]).

MS stellt das Tool „**Diagnosedatenanzeige**" zur Verfügung, mittels dem Nutzer:innen prüfen können, welche Telemetriedaten an MS weitergegeben werden – vorausgesetzt die Administration hat diese Möglichkeit frei gegeben. Schaltet man die Funktion „optionale Diagnosedaten" allerdings aus, funktionieren manche Anwendungen und deren Analyse nicht mehr. Es ist also abhängig von den betriebsspezifischen Einstellungen, ob die Nutzer:innen diese Prüfung vornehmen können – oder nicht.

Mit MS 365 ist es möglich, **Profile** über einzelne Nutzer:innen zu erstellen. MS 365 erstellt diese Profile auf Basis intransparenter Parameter (z. B. Viva [S. 52]). Die Erstellung von Profilen erfolgt, ohne dass die Informationspflichten an die Betroffenen, also die Nutzer:innen, eingehalten werden. Diese Information müsste den Zweck, den Empfängerkreis und die den Profilen zugrundeliegende Logik beinhalten.

Zudem besteht die Gefahr, dass Arbeitgeber:innen auf der Grundlage der von MS analysierten Daten, Entscheidungen über Beschäftigte treffen könnten (z. B. Karriereförderndе 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 (Artikel 22 Abs 1 DSGVO).

Es fehlt meistens eine **Datenschutzfolgenabschätzung** (DSFA) [S. 18]. 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 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 Bundesbehörden gehackt worden war. Im Juni 2024 wurde bekannt, dass MS offensichtlich der Zugangsschlüssel zur Azure Cloud verloren gegangen war. Im Juli 2024 verursachte ein Security-Update des Auftragsverarbeiters Crowdstrike weltweite Shutdowns (deutsch: Betriebsstilllegung, Stillstand, Abschaltung), unter anderem in der öffentlichen Infrastruktur. Eigentlich müsste es aber geeignete Maßnahmen geben, um Derartiges zu verhindern (Art. 25 DSGVO).

Um die Kommunikation über MS 365 zu nutzen, müssen die Betroffenen **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 Artikel 4 Z 11 DSGVO).

MS gibt **Daten europäischer Kund:innen an US-amerikanische Behörden zur Strafverfolgung** weiter. Das ist nach US-amerikanischem Recht so bestimmt. Zwar klagt MS mitunter gegen eine solche Herausgabe, muss aber dennoch zugeben „in sehr wenigen Fällen" dem Ansinnen der Behörden nachgekommen zu sein. Man muss MS zugutehalten, dass es einen detaillierten Report im Zuge der Corporate Social Responsibility erstellt.[3]

MS sieht das relativ sportlich: „Microsoft hat mehr Erfahrung mit Gerichtsverfahren als jedes andere Unternehmen." schreibt der Konzern in seinen News am 11. Februar 2021. „Einer dieser Fälle landete sogar vor dem Obersten Gerichtshof der Vereinigten Staaten. Mit dieser Arbeit kann Microsoft seinen Kunden mehr Transparenz und einen stärkeren Schutz ihrer Daten bieten."[4]

Es stellt sich die Frage, auf Basis welcher **Rechtsgrundlage** MS 365 von den Verantwortlichen, also Arbeitgeber:innen, eigentlich verwendet werden kann (siehe Art. 5 DSGVO). Die freiwillige Einwilligung ist im Arbeitsverhältnis nicht wirklich 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. Bleiben eigentlich nur mehr die „berechtigten Interessen des Verantwortlichen". Und diese gilt es zu prüfen, ob nicht „die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen".

Die deutsche Datenschutzkonferenz, der Zusammenschluss aller Landesdatenschutzbeauftragten, stellt sich bereits länger die Frage, ob die Datenverwendungen von MS DSGVO-konform sind, und kommt im Oktober 2022 zu dem ernüchternden Schluss, dass dies nicht der Fall ist. Dabei argumentiert die Datenschutz-Konferenz vor allem damit, dass die Datenverarbeitung

3 https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (Letzter Zugriff: 14.3.2025)
4 https://news.microsoft.com/de-at/neue-masnahmen-zum-schutz-ihrer-daten/ abgerufen am 5.2.2025)

seitens MS **intransparent** sei und nach wie vor **Datenübermittlungen in die USA** stattfinden.

MS selbst argumentiert, dass die Datenverwendungen „Industriestandard" seien. MS qualifiziert seine Datenverwendungen als „nötig, damit Kunden die erwünschten Vorteile der Cloud nutzen können". MS beschreibt die Rechenschaftspflicht als „ausufernde Erwartungen an Verantwortliche (...) praxisfern und blockiert technischen Fortschritt". Schließlich schreibt MS in seiner Stellungnahme: „Bei vernünftiger Betrachtung handelt es sich hier um eine rein akademische, den Interessen der Kunden in keiner Weise dienende Diskussion um (...) neutrale Verarbeitungen".[5] MS definiert also nicht nur die technischen Standards, die in seine Produkte einprogrammiert sind, sondern liefert auch die Definition von „vernünftig" und „Kundeninteressen" als Replik auf einen juristischen Befund seitens der deutschen Datenschutzbehörden.

Der Europäische Datenschutzbeauftragte hat im April 2024 die Europäische Kommission geklagt, weil diese MS Anwendungen verwendet und nicht belegen kann, dass diese mit der DSGVO konform sind. Bis Ende 2024 hätte nun die EU-Kommission vorlegen müssen, wie sie MS verwendet, sodass die DSGVO eingehalten wird. Die Kommission hat Anfang Juli 2024 ihrerseits eine Klage eingebracht. MS schloss sich der Kommission an und verklagte seinerseits den Europäischen Datenschutzbeauftragten, unter anderem wegen fehlerhafter Auslegung und Anwendung von EU-Bestimmungen.[6] Im Jänner 2025 wurde der Europäische Datenschutzbeauftragte Wojciech Wiewiórowski abgewählt.[7] Die Rechtsstreitigkeiten sind dadurch aber nicht erledigt und es bleibt abzuwarten, welche Auflagen oder Strafen folgen und ob diese auch für private Unternehmen Auswirkungen haben werden.

**Datenschutzrechtliche 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 zahlreich angebotenen Apps ist nicht immer gegeben (das Zweckbindungsgebot nicht eingehalten). 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).
- Datenschutzfolgenabschätzungen werden bloß standardmäßig, selten jedoch unternehmensspezifisch durchgeführt.
- Personenbezogene Daten aus einer Anwendung werden für diverse Zwecke in anderen Anwendungen weiterverwendet (das Koppelungsverbot nicht eingehalten)

Zusammengefasst ist also Skepsis angebracht, ob die Bestimmungen der DSGVO in vollem Umfang eingehalten werden: Es mangelt an transparenten Informationen. Es mangelt an klaren Vertragsverhältnissen. Es besteht nicht immer die Möglichkeit, Privatsphäre selbst zu gestalten („Privacy by default") bzw. sie abzuschalten (Pseudonymisierung oder „Opt-Out").

5 https://news.microsoft.com/wpcontent/uploads/prod/sites/40/2022/11/2022.11_Stellungnahme-MS-zu-DSK_25NOV2022_FINAL.pdf
6 https://www.heise.de/news/Streit-ueber-Microsoft-365-EU-Kommission-verklagt-EU-Datenschutzbeauftragten-9791143.html
7 https://www.heise.de/news/Zu-kritisch-EU-Abgeordnete-waehlen-Datenschutzbeauftragten-Wiewiorowski-ab-10246049.html

## MS 365 UND DER GESUNDHEITSSCHUTZ

Im Arbeitnehmer:innenschutzgesetz (ASchG) finden sich Bestimmungen dazu, wie eine Evaluierung – auch psychischer – Gesundheitsrisiken durchgeführt (§ 4f ASchG) und wie Informationen zum Gesundheitsschutz verbreitet werden müssen (§ 12 ff ASchG). Die Evaluierung gilt nicht ausschließlich für Gesundheitsrisiken wie Lärm, Kälte oder Schmutz, sondern auch für Faktoren, die die Gesundheit beeinträchtigen, weil sie Stress auslösen oder große Unsicherheit erwecken. Zwar beziehen sich die Vorgaben des ASchG nicht explizit auf Software von MS, jedoch sind die allgemeinen Bestimmungen auch bei MS 365 zu berücksichtigen. Die zahlreichen Kommunikationskanäle, die vielfältigen – mitunter versteckten – Überwachungsmöglichkeiten und die Verknüpfungen bei MS 365 sind durchaus geeignet, zu Verwirrung, Unsicherheit, Überlastung und Ähnlichem zu führen und damit die psychische und physische Gesundheit zu beeinträchtigen. Es bestehen folglich Ansatzpunkte für eine Arbeitsplatzevaluierung wie sie das Arbeitnehmer:innenschutzgesetz vorsieht.

Um die Risiken für die Gesundheit der Beschäftigten zu minimieren, muss der oder die Arbeitgeber:in vorbeugende Maßnahmen im Sinne des Gesundheitsschutzes ergreifen (gemäß § 4 ASchG). Diese sollten ebenfalls in einer BV festgehalten werden (z. B. Deaktivieren der Statusinformation, Begrenzen der Kommunikationskanäle, Recht auf Abschalten etc.).

### Die Gefahrenverhütung

Um beurteilen zu können, welche Maßnahmen die Gesundheit schützen, ist das **S-T-O-P**-Verfahren sehr gut geeignet. Man geht dabei entlang einer abgestuften Angabe vor, wobei die nächste Stufe erst betreten wird, wenn die vorangehende erfolglos blieb, auf der vorangegangenen nicht schon alle Zielsetzungen erreicht wurden (sogenannte „Maßnahmenverdichtung"). Beginnend bei Vorkehrungen, die auf die Arbeitsmittel bezogen sind, also im Fall von MS 365 die Software, oder über technische Vorgaben bei den einzelnen Apps, endet die Maßnahmenverdichtung mit Vorkehrungen, die auf das Verhalten der einzelnen Personen abzielen. Es gilt das Motto „**Erst die Verhältnisse ändern, dann das Verhalten**".

1. **S**ubstitution : 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). Solche Maßnahmen werden in der jeweils zuständigen Fachabteilung vorgenommen.

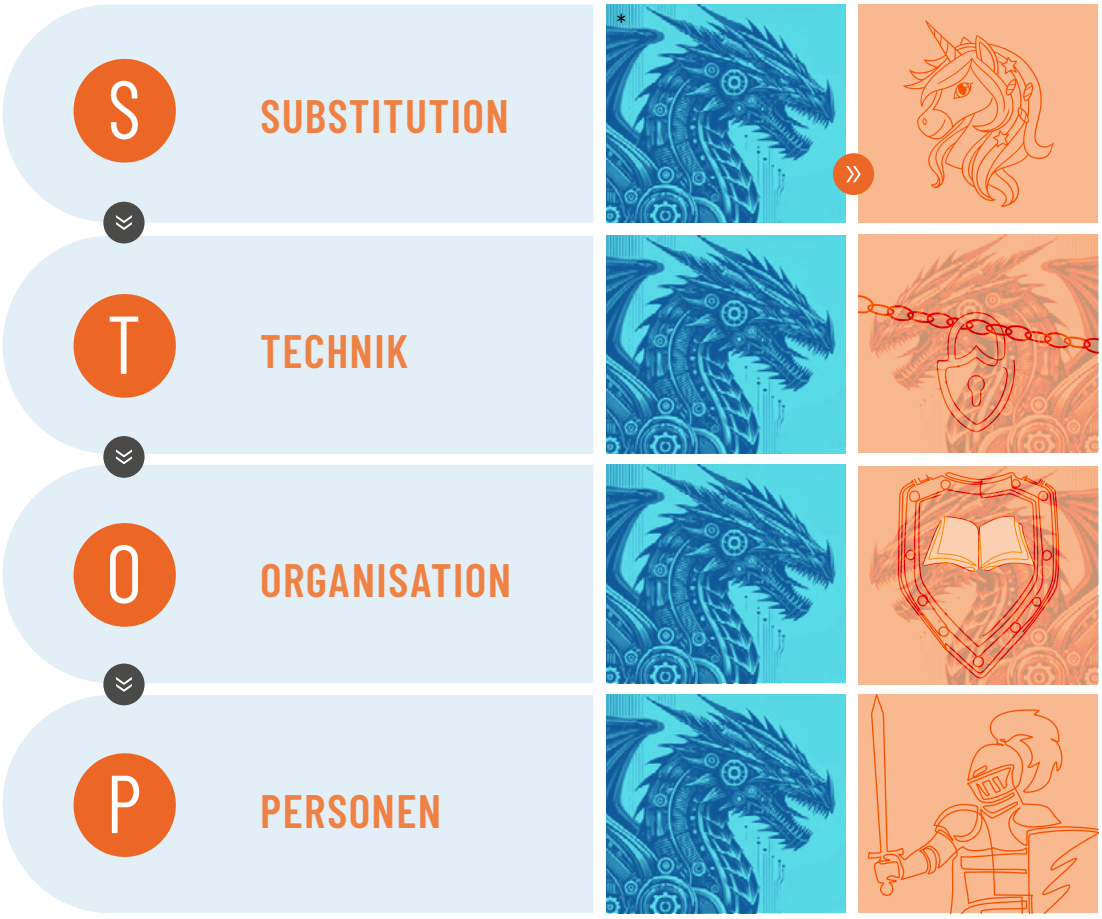
2. **T**echnik: dabei wird ein ungewünschter Zustand durch eine technisch-maschinelle Maßnahme ersetzt. Zugegebener Maßen bietet MS dafür nicht allzu viel Spielraum, die vorhandenen Möglichkeiten sollten aber gesucht und wenn gefunden, genutzt werden (z. B. eine problematische Auswertung wird anonymisiert; eine Speicherdauer wird reduziert; die Einsichtsrechte werden unterbunden, sodass die gesamte Belegschaft nicht mehr automatisch sieht, wer auf Urlaub ist, sondern man beim Versenden einer E-Mail an einen bestimmten Kollegen oder eine bestimmte Kollegin eine Abwesenheitsnotiz erhält oder Ähnliches). Diese Maßnahmen werden vorwiegend von der IT-Abteilung umgesetzt, wo beispielsweise bestimmte Anwendungen erst gar nicht freigeschalten oder Regelungen zur E-Mail-Weiterleitung, -Einsicht und Löschung eingerichtet werden.

3. **O**rganisation: Sollte eine Verbesserung auf technischer Ebene (also z. B. über Aufbewahrungsrichtlinien, sogenannte „Retention Policies") nicht möglich sein, sind organisatorische Vorgaben das Mittel der Wahl (z. B. können zwar Nutzungsauswertungen auf Teams erfolgen, doch dürfen sie von den Teamleitungen, also den „Teams-Ownern", nicht interpretiert werden oder Folgemaßnahmen nach sich ziehen; es wird zwar die „Praise"-Funktion" ermöglicht, also das Versenden lobender Emojis an Kollegen oder Kolleginnen, doch werden diese nicht erfasst und ausgewertet, geschweige denn zu Beurteilungen herangezogen). Hier wird der wichtigste Ansatzpunkt für die Verhandlung der BV liegen.

4. **P**erson: Erst wenn alle vorangehenden, auf der kollektiven Ebene ansetzenden Handlungen nicht den angestrebten Erfolg bringen, ist es angebracht, die einzelnen Beschäftigten zu Verhaltensänderungen aufzufordern bzw. individuell ein bestimmtes

# DAS S.T.O.P.-PRINZIP

## Schutz-Maßnahmen auf Basis des AschG




* Der Drache wurde mit Hilfe von Dall-E erstellt

Verhalten bei der Verwendung von MS 365-Applikationen vorzuschreiben oder zu verbieten (z. B. individuelles Abschalten von bewertenden Funktionen, individuelles Einstellen von Speicherfristen, persönliche Aufforderung zur Verhaltensänderung, Einzel-Schulung).

Obwohl dieses **S-T-O-P-Verfahren** im Rahmen des Gesundheitsschutzes entwickelt wurde, um beispielsweise Stress oder Überforderung hintanzuhalten, so eignet es sich genauso gut zum Schutz der Privatsphäre und um die Menschenwürde der Beschäftigten zu wahren.

**Die Evaluierung**

Dass evaluiert werden muss, kann sowohl aus dem ASchG abgeleitet werden als auch aus der DSGVO. Letztere sieht vor, dass eine sogenannte Datenschutzfolgenabschätzung [S. 18] durchgeführt werden muss. Während sich das ASchG auf den Schutz der Gesundheit bezieht, widmet sich die DSGVO dem Schutz personenbezogener Daten. Diese verschiedenen Ziele haben jedoch gemeinsam, dass sie eine regelmäßige Beobachtung und Anpassung des Ist-Stands erfordern. Der Betriebsrat hat also zwei gesetzliche Grundlagen, auf die er sich berufen kann, wenn die Evaluierung an das Unternehmen angepasst und gestaltet wird.

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, die Gewerkschaft GPA empfiehlt einmal im Jahr, sollte man sich unbedingt 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 wird es schwierig, so flexible und vielfältige Systeme wie die von MS 365 unter Kontrolle zu behalten.

Vor der Durchführung einer Evaluierung sollte klargestellt werden: wer sie durchführt, **wer** direkt daran beteiligt ist, **welcher Zeitraum** betrachtet wird, **welche Methoden** eingesetzt werden (z. B. Fragebogen, Interviews, Beobachtungen, Unterlagen des Arbeitsinspektorats).

Es empfiehlt sich, die Abläufe einer Evaluierung in einer Betriebsvereinbarung festzuhalten und bestenfalls auch in den Sicherheits- und Gesundheitsschutzdokumenten zu vermerken (§ 5 ASchG).

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 Z3) ArbVG)).

Im Zuge der Evaluierung sollte geklärt werden, welche maßgeblichen Veränderungen seit der letzten Evaluierung stattgefunden haben, ob es (vermehrt) zu gesundheitlichen Problemen gekommen ist und vor allem wie den aufgetretenen Problemen entgegengewirkt werden kann. Eine Erkenntnis einer Evaluierung könnte darin bestehen, dass an bestimmten Arbeitsplätzen ein Gefühl der Überwachung vorhanden ist. Abhilfemaßnahmen müssen dann jeweils auf den Betrieb, die App, den Arbeitsplatz abgestimmt sein und könnten darin bestehen, dass manche Apps durch weniger kontrollierende ersetzt werden, die denselben Zweck erfüllen („Substituierende Maßnahme"), dass manche Apps deaktiviert werden oder Darstellungen pseudonymisiert werden („Technische Maßnahme"), dass auf personenbezogene Auswertungen ausschließlich Admins für sicherheitsrelevante Zwecke zugreifen dürfen oder dass die Handhabung bestimmter Anwendungen im gesamten Betrieb deutlich geklärt wird („Organisatorische Maßnahme") dass an einzelnen Arbeitsplätzen die Schutzmaßnahmen verbessert werden oder dass vermehrt Unterweisungen an einzelne Beschäftigte in der Handhabung von Privacy-Einstellungen von MS 365 stattfinden („Personelle Maßnahme").

**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 (siehe § 14 Abs 1 ASchG). Es wird beispielsweise mit anderen Mitteln kommuniziert (z. B. Teams [S. 43], Sharepoint [S. 67], Viva Engage [S. 54]), es werden andere Mittel für die Erstellung von Dienstplänen verwendet (z. B. Planner [S. 56], Project [S. 56], Forms [S. 58]), es werden Weiterbildungen und Seminare mit digitalen Mitteln online abgehalten (z. B. Teams [S. 43], Visio [S. 61]) u.s.w.
Für Apps von MS 365, also Arbeitsmittel, ist eine Unterweisung gemäß ASchG erforderlich, zu der auch fachkundige Personen in Sachen psychische Belastungen hinzugezogen werden können. Das empfiehlt sich geradezu, angesichts der vielfältigen (neuen) 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 kommt es zu einer Überforderung, 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 regelmäßige Evaluierung von MS 365 könnte auch zu den Aufgaben einer internen MS 365-Gruppe [S. 35] zählen. Mit oder ohne MS-Gruppe, eine Evaluierung soll jedenfalls stattfinden. MS 365 wird beständig erweitert und abgeändert. Dieser Wandelbarkeit wird am besten Rechnung getragen, indem regelmäßig evaluiert [S. 23] und die BV angepasst wird.

Vom Gedanken einer für die Ewigkeit abgeschlossenen BV muss man sich bei MS 365 verabschieden.




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).

**Zum Ablauf einer Evaluierung sollten im Vorfeld einige Punkte klargestellt werden:**

- Wer ist Hauptverantwortliche/r? Wer führt sie durch? Wer wird beteiligt?
- Mit welchen Methoden wird evaluiert? Fragebogen/Interviews/Beobachtungen? Welche Hilfestellungen vom Arbeitsinspektorat werden genutzt?
- In welchen Abständen wird evaluiert?
- Die genaueren Abläufe einer Evaluierung sollten jedenfalls in einer Betriebsvereinbarung festgehalten werden.

Eine Erkenntnis einer Evaluierung könnte darin bestehen, dass an bestimmten Arbeitsplätzen ein Gefühl der Überwachung vorhanden ist. Abhilfemaßnahmen müssen dann jeweils auf den Betrieb, die App, den Arbeitsplatz abgestimmt sein und könnten darin bestehen, dass manche Apps durch weniger kontrollierende ersetzt werden, die denselben Zweck erfüllen („Substituierende Maßnahme"), dass manche Apps deaktiviert werden oder Darstellungen pseudonymisiert werden („Technische Maßnahme"), dass auf personenbezogene Auswertungen ausschließlich Admins für sicherheitsrelevante Zwecke zugreifen dürfen („Organisatorische Maßnahme") oder dass vermehrt Unterweisungen in der Handhabung von Privacy-Einstellungen von MS 365 stattfinden („Personelle Maßnahme").

# GESTALTUNG DER BASIS EINER BETRIEBS-VEREINBARUNG

## WIE MS 365 REGELN?

Bei einem 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 im betrieblichen Alltag, 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. Mit der fehlenden Zustimmung des Betriebsrats ist in der Regel der Einsatz der jeweiligen App arbeitsrechtskonform nicht mehr möglich.

Eine andere Variante wäre, dass der Betriebsrat innerhalb einer Betriebsvereinbarung bestmöglich auf die Verwendung der jeweiligen App von MS 365 Einfluss nimmt, In der BV können durch klare Regeln überschießende Leistungskontrollen der Beschäftigten unterbunden werden. Es kann das Durchleuchten der Beschäftigten hintangehalten werden, etwa, indem die Einsicht von Vorgesetzten in bestimmte personenbezogene Datenanalysen unterbunden wird.

Eine Betriebsvereinbarung ändert nichts daran, dass die grundsätzliche datenschutzrechtliche Verantwortung bei dem oder der Arbeitgeber:in liegt. Das Bestehen einer Betriebsvereinbarung ändert nichts daran, dass die EU-Datenschutzgrundverordnung (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).

MS 365 erfordert jedenfalls den Abschluss einer Betriebsvereinbarung. Sowohl einzelne Apps, 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.

Je nachdem, welches MS-Abonnement ein Unternehmen gebucht hat, beziehungsweise, welche Lizenzen ein Unternehmen gekauft hat, unterscheidet sich das Paket. Außerdem 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 Kund:innen oder/und zur Plaudern mit Kolleg:innen). Es ist also je nach Betrieb unterschiedlich, auf welche Art (wie), zu welchem Zweck (wozu), in welchem Ausmaß (wieviel) MS 365 jeweils verwendet wird.

MS 365 ist ein Gesamtpaket, das in unterschiedlichster Art und Weise in den Betrieben zum Einsatz kommt. Was genau in der Betriebsvereinbarung (BV) enthalten ist, welche Regelungen im Betrieb hilfreich sind, welcher Umgang mit den Apps passend ist, das wird je nach Branche, Betriebsgröße, Betriebskultur und vor allem je nach verwendeten MS 365 anders sein.

Bei der Anwendung von MS365 Produkten, insbesondere, wo derzeit (fast) sämtliche Apps mit KI erweitert werden, bestehen vielfältigste Kombinations- und Anwendungsmöglichkeiten. Ein Muster für eine Betriebsvereinbarung könnte diesen unzähligen Möglichkeiten nicht gerecht werden – die Gewerkschaft GPA bietet daher auch kein solches Muster an.

Was die Gewerkschaft GPA anbietet, ist die allgemeine **Rahmen-BV**, die für alle IT-Systeme verwendet werden kann. Diese erhalten in der Gewerkschaft GPA organisierte Betriebsrät:innen bei ihren Betriebsbetreuer:innen.

Was die Gewerkschaft GPA außerdem anbietet, sind die **Checklisten** im Anhang der Broschüre ([S. 86] sowie Beiheft).

Was die Gewerkschaft GPA vorschlägt, ist Anwendungen nach ihren Funktionen/ Zwecken zusammenzufassen und eine „**Funktions-BV**“ abzuschließen (siehe Bild [S. 37]).

Die Gewerkschaft gibt diese Broschüre zur Unterstützung der Betriebsrät:innen heraus, in deren ersten Teil allgemeine Vorschläge zur Gestaltung einer BV gegeben werden und im zweiten Teil zu den wichtigsten und häufigsten Apps aus der Welt von MS 365.

**Im Drei-Schritt zur Betriebsvereinbarung**

**Schritt eins**: Verschaffe dir einen Überblick über Anwendungen im Betrieb. Siehe Beiheft.

WELCHE MS 365 Anwendungen werden verwendet? lautet die Frage, die sich 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 sich der BR stellen muss.

Auf dieser Basis folgt erst **Schritt drei**: erstelle eine BV. Dabei können die Beispieltexte dieser Broschüre oder Abschnitte aus den Muster- Betriebsvereinbarungen der Gewerkschaft GPA helfen. Die Checkliste, was in einer (Basis-)Betriebsvereinbarung zu regeln ist [S. 86] hilft den Überblick zu behalten und fasst zusammen, was systemübergreifend zu den MS 365 Anwendungen zu regeln ist.

WIE soll MS 365 im Betrieb verwendet werden? lautet die Frage, die sich der BR stellen muss.

**Außerdem hilft es auf dem Weg zur BV 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 **Zeitpunkte**, Fristen, bis wann die jeweiligen Vorschläge durchgesehen werden?
- Wie sieht das **Umfeld** aus? Gibt es bereits BVen zum Thema? Müssen diese adaptiert werden? Müssen neue BVen verhandelt werden?
- Welche **Struktur** soll die BV bekommen? Soll sie ein grober Rahmen für alle Apps sein? Wird es eine Regelung für eine Gruppe von Apps, die eine gemeinsame Funktion haben (z. B. Kommunikation, Security)? Soll eine einzelne App (z. B. Teams) geregelt werden? Soll eine einzelne Funktion (z. B. Standorterfassung, Privatnutzung) geregelt werden? Was sind die wesentlichsten Punkte, die vereinbart werden müssen?

Es hilft beim Arbeiten mit MS 365 einige grundlegende Prinzipien zu beachten, unabhängig davon, welche Lizenzen, Apps, erweiterten Services etc. genutzt werden.

Worauf soll das Augenmerk gelegt werden, wenn eine allgemeine Basis- Betriebsvereinbarung zu MS 365 ausverhandelt wird? Folgende Punkte gilt es generell beim Abschluss einer Betriebsvereinbarung zu bedenken:

## DER VERWENDUNGSZWECK

Der **Zweck** muss eindeutig sein. Das ist eine Grundregel aus der Datenschutzgrundverordnung (DSGVO). Es muss klar ersichtlich sein, welche Daten wofür verwendet werden. Die Zweckbindung kann allgemein formuliert werden.

In der hier zitierten Betriebsvereinbarung wurde der Zweck auch hinsichtlich der Rahmen-BV selbst formuliert, was durchaus sinnvoll sein kann, um gegenüber der Geschäftsführung die Wichtigkeit einer solchen Basis-Betriebsvereinbarung hervorzuheben, die rein rechtlich nicht zwangsläufig erforderlich ist.

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 werden im Folgenden die Zwecke, zu denen Beschäftigtendaten mit M365 verarbeitet werden dürfen, festgelegt:

- zur Bereitstellung und Nutzung von M365 die technisch erforderlichen Nutzer:innendaten ;

- zur Unterstützung der Kommunikation und Zusammenarbeit in den einzelnen Teams des/der Arbeitgebers:in;
- zur Umsetzung und Kontrolle von Datenschutz und IT-Sicherheit;
- zur Dokumentation des/der zuständigen Bearbeiters:in 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 zur regeln.

**Ziel dieser Rahmenbetriebsvereinbarung ist 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 von personenbezogenen Daten zu unterbinden.

Für einzelne Anwendungen soll der Zweck wozu sie verwendet werden, klar dargestellt werden (z. B. Speichern von Sprachnachrichten bei Gesprächen mit Kundinnen und Kunden mit dem Zweck, gesetzliche Haftungsansprüche klären zu können).

Die Einstellung „optional verbundene Erfahrungen" (optional connected expiriences) kann dazu führen, dass getroffene Datenschutzbestimmungen unterwandert werden. Im Entra ID [S. 78] können die „optionalen Erfahrungen" deaktiviert werden, womit unerwünschte Datensammlungen unterbunden sind. Damit fallen allerdings auch andere automatisierte Auswertungen weg (z. B. das Einbinden von zusätzlichen Anwendungen (auch AdIns genannt) oder des Copilot-Store).

## DIE ZUGRIFFSBESCHRÄNKUNG

Aus der Zweckbindung ergibt sich, wer welche **Berechtigung** erhalten muss. Dass möglichst wenige Daten nur jenen, die sie für ihre Arbeitsaufgaben benötigen zu Verfügung stehen sollen, ergibt sich aus der DSGVO-Grundregel der **Vertraulichkeit** sowie der Datenminimierung. Ist der Zweck beispielsweise das Vermeiden von Virenbefall, sind IT-Administratoren und -Administratorinnen diejenigen, die eine Berechtigung brauchen. Berechtigungskonzepte sind restriktiv zu fassen, damit die ohnehin eng verflochtenen Datenkombinations- und Auswertungsmöglichkeiten keine privaten Einblicke in das Verhalten und die „Leistung" der Beschäftigten beinhalten. Im Standard-Berechtigungskonzept von MS 365 sind etwa 100 Rollen vorgesehen, die in weitere untergliedert werden können.

Der Betriebsrat selbst braucht eine Rolle, damit er überprüfen kann, ob das Rollenkonzept stimmig ist und ob die Vorgaben auch eingehalten werden.

Änderungen des Berechtigungskonzeptes kommen häufig vor (z. B. Personaländerungen). 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 M365. Zusätzlich erhält der Betriebsrat Zugriff auf ein Auditierungswerkzeug mit Leserechten für das Nachvollziehen der Konfigurationseinstellungen sowie der Aktivitäten der Administrations-User in dem M365 Produktiv-Mandanten.

## DIE SPEICHERDAUER

Manche Auswertungen in MS 365 bauen auf langfristig auswertbaren personenbezogenen Datenhistorien auf (Delve [S. 61]). Die gesetzliche Grundregel für **Löschfristen**, wonach personenbezogene Daten nur so lange aufbewahrt werden dürfen, als sie ihren Zweck erfüllen, wird dadurch konterkariert. Innerbetrieblich muss daher 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 wäre, sämtliche technischen Möglichkeiten auch praktisch umzusetzen. „Technisch möglich – organisatorisch untersagt" sollte der Wahlspruch lauten. Das ist schon allein deshalb wichtig, damit man das Prinzip der „Datenminimierung" (gemäß Art 5 Abs 1 c DSGVO) einhält und damit „technische und organisatorische Maßnahmen" (gemäß Artikel 32 DSGVO) getroffen werden.

## DIE PRIVATNUTZUNG

Da MS 365 (fast) immer auch ein Werkzeug für Kommunikation und Zusammenarbeit ist und nahezu jederzeit und von überall erreichbar ist, fordert es ein extensives Arbeiten geradezu heraus. E-Mails werden vor dem eigentlichen Arbeitsbeginn gelesen, Dokumente nach Arbeitsende bearbeitet ... MS 365 bietet einige Apps an, die zur Kommunikation genutzt werden können (z. B. Outlook [S. 41], Teams [S. 43], Viva Engage [S. 54] etc.). Das kann – insbesondere bei der Einführung, wenn die verschiedenen Möglichkeiten noch nicht erprobt und eingeübt sind – zu Verwirrung und Überforderung führen.

Eine Abgrenzung von beruflicher und **privater Nutzung**, eine Begrenzung der Kommunikationskanäle sowie das „Recht auf Abschalten" sind daher angebracht.

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

MS 365 ermöglicht eine Nutzung, die weit über betriebliche Zwecke hinausgeht. Daher sollte der oder die Arbeitgeber:in klar kommunizieren, was in der Arbeitszeit verboten ist (z. B. Games, Unterhaltungsserien, Shoppen) und was erlaubt ist. Für die Privatnutzung sollte festgelegt sein, wo gespeichert wird (z. B. verlangen manche Firmen, dass private Daten nur lokal im Gerätespeicher gelegt werden dürfen, betriebliches nur in der dafür vorgesehenen OneDrive [S. 60]).

Eine Menge Apps und Plattformen stehen im Rahmen von MS 365 zur Verfügung. Zusätzlich bietet MS 365 **Schnittstellen** zu externen Programmen (z. B. der Spiele- und Softwareplattform „Steam" oder der Videokonferenztool Webex vom US-amerikanischen Konzern Cisco), womit sich das Angebot schier unendlich erweitert, ohne dass der oder die Nutzer:in den Eindruck hätte, die Welt von MS 365 zu verlassen. Auf all diesen Applikationen, Anwendungen und Softwareprodukten können sämtliche Aktivitäten der Nutzer:innen gespeichert, nachverfolgt und ausgewertet werden. Somit können tiefgreifende, in die Privatsphäre reichende Persönlichkeitsprofile erstellt werden.

## DIE PROFILE

Damit die unzähligen Auswertungsmöglichkeiten von MS 365 nicht zu Lasten der Beschäftigten gehen, sollte der Schutz der Beschäftigten vor einer überschießenden Überwachung in einer BV festgehalten werden. Das gelingt, indem Vorgesetzte auf die Analyse von Leistungs- oder Verhaltensprofilen keinen Zugriff haben. Insbesondere grafische Anzeigen des Arbeits- bzw. Erledigungsstands der Kollegen und Kolleginnen

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" Kolleg:innen – eventuell ergänzt mit einem Erlaubnisvorbehalt – sollte daher in der BV enthalten sein.

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

Jegliche Art der Verarbeitung personenbezogener Daten, beispielsweise zur Bewertung der persönlichen Aspekte eines Mitarbeitenden insbesondere zur Analyse oder Prognose von Aspekten bezüglich seiner/ihrer Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönlicher Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel ausgeschlossen (Profilingverbot).

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.

Auf vielen MS Anwendungen können die Nutzer:innen eigene Profile anlegen (z. B. MS-Teams [S. 43], Sharepoint [S. 67]). Die Freigabe persönlicher Informationen (z. B. Profil-Foto, Verfügbarkeitsstatus, Kontakte ...) sollte aber immer freiwillig sein. Die Verweigerung der Freigabe darf keine negativen Konsequenzen für Beschäftigte haben. Also empfiehlt es sich generell, ein Benachteiligungsverbot zu vereinbaren.

## DIE KONTROLLMASSNAHME

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.

Wurde 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, wird der oder die Vorgesetzte und ein Mitglied des Betriebsrates informiert und ein ehestmöglicher Gesprächstermin vereinbart.

Auf Wunsch des oder der 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 disziplinäre 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] vorliegen. In derartigen Notfällen wird die Ausgangslage konkret begründet und es darf das Konfliktlösungsgespräch unterbleiben bzw. erfolgt erst, wenn die Sicherheit des Betriebs wieder gewährleistet ist. Der oder die 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 informiert, wie viele derartige Gespräche stattgefunden haben.

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

In einer Muster-Betriebsvereinbarung eines deutschen Rechtsanwalts findet sich folgender Formulierungsvorschlag:

Zur Klärung schwerer arbeitsrechtlicher Pflichtverletzungen, die gleichzeitig eine Straftat darstellen, darf bei begründetem, auf Tatsachen beruhenden, dokumentierten Verdacht der/die 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.

## DIE SCHULUNG

Zu jeder in Betrieb befindlichen Anwendung ist unbedingt eine Schulung anzubieten. Vor allem in der ersten Einführungsphase sind Trainer:innen, Lernbegleiter:innen, Buddies, Mentor:innen, Experten und Expertinnen für die Beschäftigten von großem Nutzen. In einigen Betrieben werden sogenannte „Champions“ ernannt, die als Ansprechpersonen zur Verfügung stehen [S. 34]. Bei den Schulungen ist es einerseits sinnvoll, die direkte Anwendung und die vielfältigen Möglichkeiten der eingesetzten Apps von MS 365 zu erlernen, andererseits sollten auch datenschutzrelevante Inhalte in die Schulungen mit einfließen (z. B. wie Anzeigen oder Analysen unterbunden werden können, 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 prinzipiell 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 Präsenzschulungen, Webinaren oder als Selbststudium erfolgen. Die Schulungskosten trägt der oder die 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.

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 / den Mitarbeitenden veranlassen.

## DIE EINFÜHRUNG UND DIE AKTUALISIERUNG

Gerade in der Einführungsphase erfordert es viel Zeit, den Umgang mit den MS 365 Produkten zu erlernen, sich die Prozesse einzuprägen und reibungslos anzuwenden. Im Einführungsprozess sollte nicht alles auf einmal freigeschalten werden und die alten Systeme nicht von einem Tag auf den anderen abgedreht werden.

Werden neue Apps der MS-Welt hinzugefügt (z. B. Copilot [S. 62]), ist es sinnvoll, eine erste Test-Phase laufen zu lassen, für die noch keine fertige BV vorliegen muss. Während dieser Testphase kann der BR feststellen, welche Punkte besonders heikel sind und daher genau in einer BV geregelt werden müssen. Microsoft spricht diesbezüglich von einer „**Toleranzphase**" (bzw. bei Copilot von einem „Copilot-Lab"), da BV-pflichtige Apps im Einsatz sind, ohne dass eine solche BV unterschrieben ist. Klar sein muss dabei, dass eine solche Toleranzphase ein Ablaufdatum hat.

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

Dass der Betriebsrat eingebunden wird, sollte jedenfalls in der Basisbetriebsvereinbarung festgehalten werden. Dazu ein gekürzter Vorschlag eines deutschen Technologieberaters:

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 ggfs. 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 Customisingphasen, 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.

**Zu den Updates sollten folgende Vereinbarungen getroffen werden:**

Die BV sollte befristet abgeschlossen werden, womit die Möglichkeit besteht, sie an aktuelle Veränderungen anzupassen bzw. wenn keine relevanten Veränderungen vorliegen, die BV zu verlängern.

„Targeted release" kann für ausgewählte Benutzer:innen eingerichtet werden, um vorab zu testen, was es Neues gibt Updates können also vor Freigabe in einem sicheren separaten Bereich getestet werden und die Testergebnisse mit dem BR besprochen werden.

In einer solchen Testgruppe sollten folgende Fragen besprochen werden:

- Tangiert das Update die Speicherung von Beschäftigtendaten?
- Tangiert das Update die Auswertung von Beschäftigtendaten bzgl. Leistungs- und Verhaltenskontrolle?
- Ändert sich durch die Updates die Arbeitsorganisation/Zusammenarbeit (z. B. durch permanente Anzeige des Präsenzstatus, automatische Übernahme von Terminanfragen aus Teams)?
- Hat das Update Auswirkungen auf die Qualifizierung der Beschäftigten (z. B. Trainingserfordernisse)?
- Sind die Einstellungen im Admincenter nach dem letzten Update noch so, wie sie es zuvor waren?

Aktualisierungen/Updates werden regelmäßig von MS geliefert. Nicht immer gelingt es, einen Überblick über sämtliche Änderungen von MS-Produkten zu behalten – geschweige denn, die Updates vorab einer Prüfung zu unterziehen. Ein Betriebsrat beschreibt seinen Eindruck dieser raschen Wechsel von MS 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. Das ist, wie wenn im Supermarkt die Regale umgeräumt werden. Da kannst du nix dran ändern."

Die neuesten Freigaben stellt MS 365 auf einer eigenen Webseite übersichtlich gegliedert nach Lizenzmodell und Produkt dar: h**ttps://www.microsoft.com/en-us/microsoft-365/roadmap** Es lohnt sich regelmäßig nachzusehen, um auf dem Laufenden zu bleiben welche Veränderungen, welche neuen Möglichkeiten von MS veröffentlicht werden (Englisch: Releases).

## DIE ANSPRECHPARTNER:INNEN

Manche Betriebe ernennen auf Anraten von Microsoft bei der Einführung von MS 365 „**Champions**". In anderen Betrieben nennt man diese Ansprechpersonen „Power-User:innen" oder „Key-User:innen". Sie sind in der Regel aus dem Kreis der Kolleg:innen, also der „normalen" Nutzer:innen und werden eigens zu den unterschiedlichen Anwendungen von MS 365 geschult bzw. von der täglichen Arbeit freigestellt, um die Apps besser kennenzulernen, sie besser zu durchschauen, mit den Apps zu „spielen". Sie bringen idealerweise Interesse an technischen Abläufen und Neugierde mit. Geduld und didaktisches Geschick ist ebenso von Vorteil. „Champions" sollen ihre Kenntnisse an die Belegschaft weitergeben. Wenn Unklarheiten auftauchen, soll der oder die Beschäftigte sich nicht sofort an den Helpdesk wenden, sondern zuerst bei den Champions nachfragen, ob ihm oder ihr eine Lösung einfällt. Der Nachteil an dem Konzept ist, dass Champions eine Verantwortung übertragen bekommen, die schwierig zu erfüllen ist. „Champions sind nichts anderes als billige Hilfskräfte für die Geschäftsführung, damit die sich umfassende Schulungen für alle ersparen." behaupten kritische Geister. Andere wiederum empfinden die Kolleg:innen als äußerst hilfreich, kompetent und vor allem notwendig. Es wird wohl darauf ankommen, wie genau diese Ansprechpersonen selbst Bescheid wissen und ob sie eigenständig handeln und unterstützend tätig werden können.

MS 365 ist ein sehr flexibles und schnelllebiges Programm, das daher auch einer ebenso flexiblen und

flotten Auskunftsstelle bedarf. Idealerweise stehen auch nach der Ausrollung und ersten Einschulung **Ansprechpartner:innen** zur Verfügung, die jederzeit auftretende Fragen beantworten können. Für Fragen aus der Belegschaft betreffend MS 365 braucht (meist) auch der Betriebsrat eine solche Ansprechperson. Diese kann behilflich sein, falls der Betriebsrat Änderungsbedarf an der BV sieht. Eine solche bedarfsorientiert anwesende Stelle könnte auch in die BV aufgenommen werden.

Bei einer umfassenden Software wie MS 365 wird man mit einer Person, die sich auskennt, nicht das Auslangen finden. Eine eigene, mit möglichst fixen Mitgliedern zusammengesetzte „**interne Microsoft-365-Datenschutzgruppe**", die aus Beschäftigten unterschiedlicher Bereiche sowie Fachexperten und -expertinnen besteht (z. B. IT, HR, Recht, Betriebsrat, Vertrieb, Produktion, Geschäftsführung, betriebliche Datenschutzbeauftragte oder betrieblicher Datenschutzbeauftragter, externe Sachverständige), sich möglichst regelmäßig trifft und die sich der Fragen in Zusammenhang mit MS 365 annimmt, ist eine hilfreiche Sache. Manche Betriebe nennen eine derartige Gruppe „gemeinsamer MS 365-Ausschuss" oder „Kommission". Zusammensetzung, Aufgaben, Frequenz der Treffen und Entscheidungsbefugnisse dieser Gruppe können in einer BV festgehalten werden.

Aufgrund der schnellen technologischen Entwicklung bezieht sich diese Betriebsvereinbarung (BV) auf den IST-Stand der Systeme und gesetzlichen Regelungen zum Stichtag ..... 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.

Zur Evaluierung der Bestimmungen der Vereinbarung, zur Analyse der organisatorischen und technischen Veränderungen sowie als Anlaufstelle für betriebliche Erfahrungen im Umgang mit Microsoft 365 wird eine prozessbegleitende IT-Arbeitsgruppe gebildet. Treffen finden zumindest zwei Mal pro Jahr statt. [vierteljährlich wäre auch eine gute Option; Anm. GPA] Diese Arbeitsgruppe unterstützt die Arbeitgeber:in in ihrer/seiner Rolle als datenschutzrechtlich Verantwortliche in der Ausarbeitung von transparenten Informationen an die von der Datenverarbeitung betroffenen Beschäftigten und berät diese bei der Gestaltung von Schulungskonzepten.

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 (1st Level Support)
- Abteilung Recht
- Betriebsrat
- Datenschutzbeauftragte:r
- Geschäftsführung
- Im Bedarfsfall externe Beratung]

**Die einzelnen Anwendungen und der Überblick**

Um Zusatz-Betriebsvereinbarungen zu einzelnen Apps oder deren Funktionen abzuschließen, muss ein Überblick bestehen, welche Teile von MS 365 verwendet werden (siehe Beiheft). Ist unklar, welche genau im Einsatz sind, drehen sich BV-Verhandlungen gegenstandslos im Kreis. Zu den aktiven Anwendungen kann, aufbauend auf einer Basis-BV, die jeweils passende Musterbetriebsvereinbarung der Gewerkschaft GPA als Inspirationsquelle für konkrete Formulierungen herangezogen werden. Die Gewerkschaft GPA bietet zahlrei-

che Muster-BVs zu einzelnen Systemen an, wie bspw. zu E-Mail/Internet (die passende App dazu ist Outlook [S. 41], Telefon (die MS-App für diesen Zweck ist Phone auf Teams), Videokonferenzsysteme (dazu dient Teams [S. 43], Mobile Device Management (dies wird in den meisten Betrieben mit Intune gemacht [S. 80] etc. Für die einzelnen Anwendungen sollte dann konkret vereinbart werden, wie und wofür sie genutzt werden. Um sich dabei nicht zu wiederholen, können die allgemeinen Punkte in einer Rahmen-Betriebsvereinbarung zusammengefasst werden.

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

> Apps, die nicht in der Systembeschreibung in der Anlage aufgeführt sind, sind im Tenant für die Nutzer:innen der österreichischen Standorte zu deaktivieren.

Anm.: In einem Microsoft 365 Tenant sind alle Dienste, Daten und Konten (in der Cloud) zusammen gespeichert. Dadurch soll sichergestellt werden, dass Informationen nicht versehentlich mit anderen Unternehmen geteilt werden. Man kann sich den Tenant wie ein virtuelles Gebäude für ein Unternehmen (oder eine:n anderen Kund:in) vorstellen, in dem alle Räume untergebracht sind.

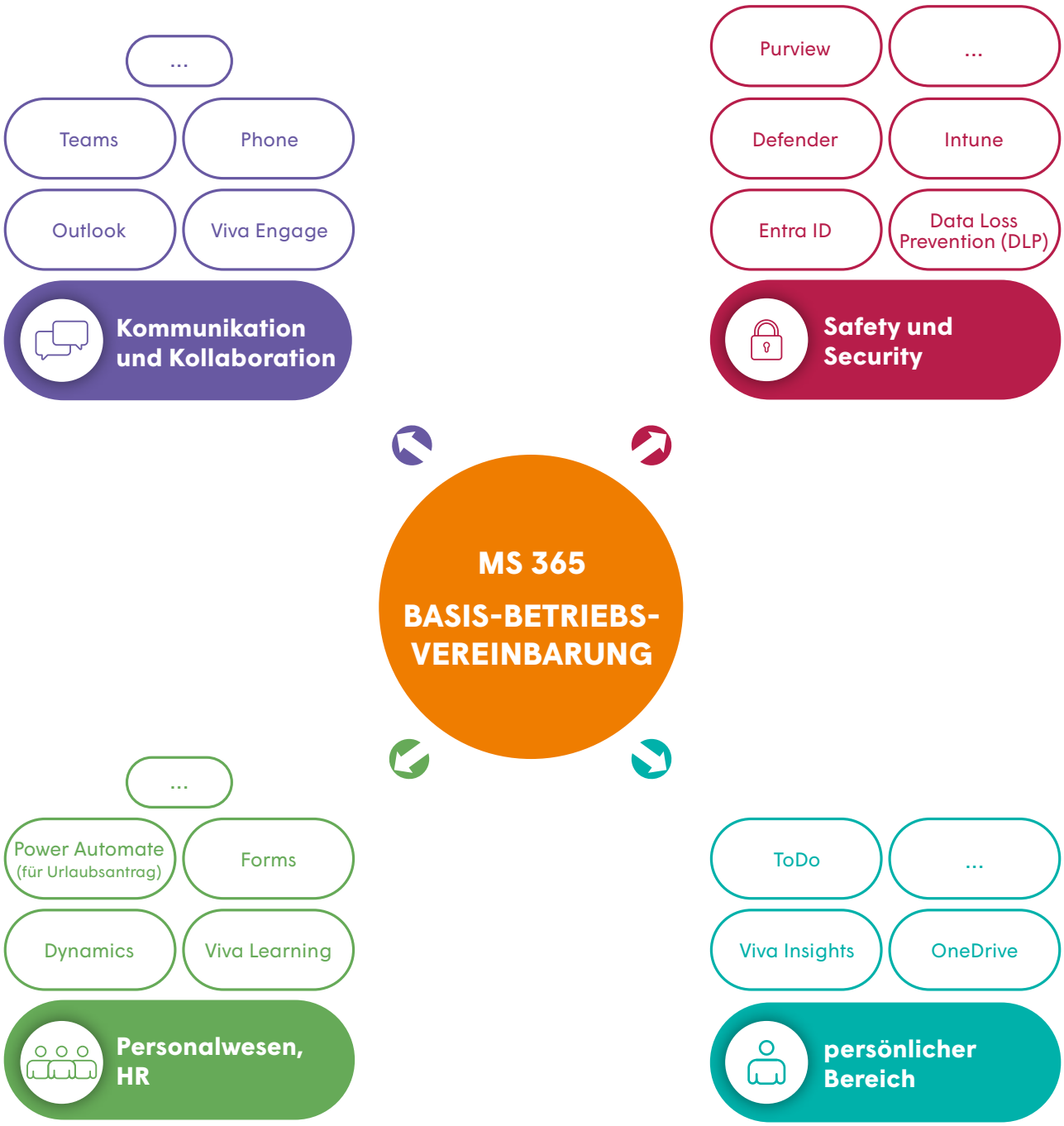
**Zusammenfassung der wichtigsten Regelungspunkte in einer Basis-Betriebsvereinbarung zu MS 365** (siehe auch Checkliste im Anhang [S. 86])**:**

- Zweck möglichst genau angeben
- Berechtigungskonzept erstellen (= Zugriffskonzept, Rollenkonzept); Einsichts- und Kontrollrechte für den BR festlegen
- Auswertungs- und Überwachungsmöglichkeiten beschränken
- Löschkonzept erstellen
- Privatnutzung regeln
- Freiwilligkeit festlegen wo möglich
- Schulungsplan erstellen (inkl. Schulung zu Privatsphäre schonende Einstellungen)
- Ansprechpersonen definieren, MS 365 Experten- und Expertinnen-Gruppe installieren
- Vorgehensweise bei Updates vereinbaren (= Aktualisierungen, Releases, Verbesserungen)
- Vorgehensweise bei Kontrollmaßnahmen bzw. Fehlverhalten vereinbaren (= „stufenweise Kontrollverdichtung“)
- Regelmäßige Evaluierung durchführen (inklusive der Risiken für die Privatsphäre sowie der Gesundheitsrisiken)

Das Regeln der Verwendung vieler unterschiedlicher Systeme und mannigfaltiger Beschäftigtendaten im Betrieb könnte am besten mit Hilfe der „**Rahmen-Muster-BV Datenschutz**“ klappen. Diese Rahmen-BV der Gewerkschaft GPA enthält Datenschutzregelungen, die für sämtliche Systeme gelten (z. B. der Umgang mit Protokolldaten, also Log-files, die in allen Systemen anfallen) und ist bei den Regionalsekretären und -sekretärinnen erhältlich. Die zum Betrieb passende Betriebsvereinbarung muss selbst zusammengestellt werden, so wie auch jeder Betrieb aus den unterschiedlichsten MS 365 Anwendungen ein eigenes System „zusammenpuzzelt“.

MS 365 deckt ein sehr weites Spektrum an betrieblichen Aufgaben ab, wobei diese alle eng miteinander verzahnt sind und nicht immer eindeutig voneinander abgegrenzt werden können. Um sich daran anzupassen, ist ein **Vorschlag zur Struktur der Betriebsvereinbarung** (s. Grafik [S. 36]), die verschiedenen Apps nach Funktionen zusammenzufassen (z. B. Kommunikation, Sicherheit, Projektmanagement etc.). Das hätte den Vorteil, sich nicht zu sehr mit einzelnen Apps aufzuhalten und sich gleichzeitig nicht zu häufig zu wiederholen, wenn zwei Apps denselben Zweck erfüllen. Welche Vorgehensweise, welche Struktur gewählt wird, muss das Betriebsratsgremium entscheiden.

## BEISPIEL EINER STRUKTUR FÜR MS365-BETRIEBSVEREINBARUNGEN



# ANWENDUNGEN FÜR NUTZER:INNEN

## EINE AUSWAHL AUS DEM FRONTEND

Im folgenden Teil der Broschüre werden jene Anwendungen von MS 365 skizziert, die in den Beratungen der Gewerkschaft GPA häufig auftreten, weithin bekannt sind und in zahlreichen Betrieben zum Einsatz kommen, etwa die extrem rasch weiterentwickelte und ausgebaute Plattform Teams [S. 43]. Außerdem sind Anwendungen dargestellt, die Besonderheiten aufweisen, wie beispielsweise ein besonders hohes Überwachungspotential bei Dynamics [S. 57] oder Viva [S. 52]. Das Paket MS 365 umfasst wesentlich mehr Programme als in dieser Broschüre angeführt sind, wie die Checkliste zu den Anwendungen im Beiheft oder ein Blick auf den „Service-Katalog" von MS 365 zeigen.

Je nach Kundengruppe (Privathaushalt, Schule, Konzern oder Klein- und Mittelunternehmen) bietet MS einen Überblick über sein Angebot
*https://www.microsoft.com/de-at/microsoft-365*

Für größere Unternehmen mit der Lizenz E3 oder E5 („E" steht für Enterprise, also Unternehmen) stellt der passionierte IT-Experte Aaron Dinnage regelmäßig eine äußerst hilfreiche Übersicht zusammen:
*https://m365maps.com/files/Microsoft-365-Enterprise-All.htm*
Ebenso zu den ergänzenden Anwendungen
*https://m365maps.com/files/Related-Services.htm*

MS 365 soll ein Produkt für alle betrieblichen Anforderungen bieten, *eine* Plattform, *eine* „Lösung", wie es in der IT oft heißt, ein „Service" wie es im Verkauf oft heißt. Man kann die verschiedenen Anwendungen grob nach den drei Gruppen von Nutzer:innen unterteilen, an die sie sich hauptsächlich richten.

1. Jene, die die einzelnen Nutzer:innen individuell verwenden. Dazu dient als persönliches Ablagesystem hauptsächlich **OneDrive**.

2. Jene, mit denen die verschiedenen Einheiten eines Unternehmens, beispielsweise Abteilungen, Gruppen, Teams, Standorte etc. zusammenarbeiten. Dazu dient vorwiegend **Teams**.

3. Und schlussendlich jene, mit denen die Leitung eines Unternehmens bzw. die damit im technischen Sinne beauftragten Administrator:innen den Gesamtbetrieb managen, die Abläufe festlegen und die Sicherheit überwachen. Dazu wird meist die Plattform **Sharepoint** bzw. für Sicherheitsrelevantes **Purview** verwendet.

Im Hintergrund sind die Anwendungen miteinander verbunden. Was Einzelne in ihren persönlichen Bereich stellen, kann beispielsweise in Teams synchronisiert, also zeitgleich freigegeben werden und wird außerdem über Sharepoint verwaltet.

Ein und dieselbe Aufgabe kann bei MS 365 mit Hilfe mehrerer Apps erledigt werden. So kann beispielsweise



sowohl der Planner [S. 56] als auch ToDo [S. 55] oder ein Channel in Teams [S. 43] für das Projektmanagement verwendet werden, um Aufgaben zu verteilen oder einen Zeitablauf festzulegen.

Ein Ablagesystem zu verwalten, ist in mehreren MS 365 Apps möglich. Geeignet sind sowohl OneDrive [S. 60], Teams [S. 43] und dessen einzelne Channels als auch Sharepoint [S. 67]. Alle diese Apps bieten eine Art Bibliothek.

Wenn im Unternehmen nicht geklärt ist, welche Kommentare, Beiträge, Nachrichten, Posts etc. in welcher App, von wem, gemacht werden sollen, oder dürfen, oder müssen, ist nicht klar, wie mit den Apps umzugehen ist. Ist ein Kommentar einer Vorgesetzten auf ToDo ein Vorschlag oder eine Arbeitspflicht? Ist eine neue Aufgabe in Planner eine Anregung oder eine wichtige Aufgabenzuteilung? Ein wesentlicher Teil der Praxis mit MS 365 besteht darin, die verschiedenen Apps so zu nutzen, dass den Beschäftigten klar ist, welche App zu welchem Zweck im Einsatz ist.

Zur besseren Übersicht sind die hier dargestellten Anwendungen unterteilt in solche für „normale“ **Nutzer:innen** und solche, die eher für **Administrator:innen** gedacht sind. Die Grenzen sind fließend, da mitunter Anwendungen für System-Administrator:innen ebenso Nutzer:innen zur Verfügung stehen.

Zur besseren Übersicht ist Wichtiges und Praktisches in grauen Kästchen hervorgehoben

Graue Kästchen mit einem Anführungszeichen beinhalten Beispiele aus bestehenden Betriebsvereinbarungen.

Kästchen mit Pfeilchen enthalten praktische Tipps.

Kästchen mit Diamanten Besonderheiten.

Am Ende jedes Kapitels sind die wichtigsten Punkte, die in einer allfällig erforderlichen Betriebsvereinbarung enthalten sein sollten, aufgezählt.

## WORD, EXCEL, POWERPOINT (VORMALS OFFICE)

Office ist das wohl bekannteste Paket von MS. Die verschiedenen Anwendungen dienen dem Verfassen von Dokumenten (Word), dem Erstellen und Berechnen von Tabellen (Excel) und dem Anfertigen von Präsentationen (Powerpoint). Eigentlich könnte man meinen, dass dies eine „harmlose" Software sei. Doch wie bei vielen Programmen, kommt es auch hier darauf an, wie es eingesetzt wird, womit verknüpft wird oder wer Zugriff hat, um die Harmlosigkeit beurteilen zu können.
Word erfasst personenbezogene Daten, die Auskunft über das Verhalten der Nutzer:innen geben. Wer hat das Dokument erstellt? Wer hat wann welche Änderungen vorgenommen? Diese und andere Informationen werden gespeichert und können zur Verhaltensanalyse herangezogen werden. Diese Versionen, sozusagen die „Lebensgeschichte" jeder Datei, wird von Word mehrmals gespeichert, abhängig von verschiedenen Faktoren wie der Speicherkapazität. Die Anzahl der Versionen ist nicht individuell einstellbar auch nicht von Admin Seite. Die Historie in MS 365 Lizenzen für Haushalte oder Einzelpersonen umfasst standardmäßig 25 Dokumente. Bei Businesslizenzen, wie sie von Unternehmen meist genutzt werden, sind Dateien wie Word, Excel oder Powerpoint, so sie auf Sharepoint [S. 67], Teams [S. 43] oder OneDrive [S. 60] abgelegt werden, automatisch in sämtlichen Versionen gespeichert. Die Anzahl der gespeicherten Versionen und die Dauer der Aufbewahrung lässt sich von den Administrator:innen in den Einstellungen zur Versionsverwaltung konfigurieren.

Darüber hinaus schreibt Graph [S. 69] im Hintergrund immer mit und verknüpft die Daten mit denen aus anderen Anwendungen.

Office bietet eine Liste **empfohlener Dateien** auf der Startseite von Word, Excel oder PowerPoint an. Damit soll den Nutzer:innen geholfen werden, auch die Arbeit – anderer Kolleg:innen – nachzuverfolgen und schnell auf Dateien mit Aktivitäten zuzugreifen, die für sie wichtig sein könnten. MS schreibt: „Dieses Feature verwendet maschinelles Lernen, um vorherzusagen, an welchen Dateien Sie am ehesten als Nächstes arbeiten möchten, (...) Es werden nur Dateien vorgeschlagen, auf die Sie in OneDrive oder SharePoint Zugriff haben." Nutzer:innen können entweder einzelne Dokumente aus der „Empfohlen" Liste entfernen, sodass sie für sie selbst nicht mehr aufscheinen (im System und damit für andere aber sehr wohl noch vorhanden sind) oder sich die gesamte Rubrik nicht mehr anzeigen lassen (wonach sie für andere Nutzer:innen dennoch sichtbar bleiben).

Ferner werden standardmäßig sogenannte Telemetriedaten (z. B. Häufigkeit, Dauer, allfällige Problemberichte) automatisch an den US-amerikanischen Mutterkonzern bzw. dessen europäische Hauptniederlassung in Irland übermittelt. Damit soll der Systemzustand festgehalten, allfällig auftretende Fehler erkannt und das System verbessert werden.

Diese Datenübermittlung kann nicht abgeschaltet werden, zählt aber nicht immer zum „berechtigten Interesse" der Kund:innen bzw. der Unternehmen, die Outlook nutzen (siehe MS 365 und der Datenschutz [S. 16]). Dazu muss es eine Information an die Betroffenen, also die Beschäftigten, geben. In einem Betrieb wurde diese Information so formuliert:

**Es besteht Regelungsbedarf:**

- Speicherort im Betrieb, innerhalb der MS Landschaft, festlegen (Wo werden gemeinsam bearbeitete Dokumente abgelegt? Wo werden besonders schützenswerte Daten (nicht) abgelegt?)

- Berechtigungskonzept festlegen (wer hat worauf Zugriff?)

- Speicherdauer festlegen (wie lange müssen welche Dokumente aufbewahrt werden?)



- Interpretationen zu Arbeitsleistung und Verhalten weitestmöglich unterbinden, arbeitsrechtliche Maßnahmen ausschließen

- Klassifikation der Dateien nach ihrer Geheimhaltungsstufe (damit einhergehend Zugriffsrechte und Speicherdauer)

- Kann die Übermittlung der Telemetriedaten an Microsoft eingeschränkt werden? (MS 365 übermittelt Diagnosedaten wie z. B. letzte Softwareupdates, Fehlerdokumentation, Anwendungsdauer, Nutzungshäufigkeit, Verbindungsunterbrechungen, Geschwindigkeit der Übermittlung, Datenschutzeinstellungen etc. an Microsoft [S. 40]).

## OUTLOOK (= E-MAIL, KALENDER, KONTAKTE)

Outlook verwaltet Termine, E-Mails und Postfächer, Adress- und Telefonnummern. Diese im betrieblichen Alltag notwendigen Anwendungen, kombiniert mit viel Speicherplatz und Vernetzungsmöglichkeiten machen Outlook zu einem der am häufigsten eingesetzten Software-Pakete.

Bei der **E-Mail-Funktion** von Outlook müssen im Hintergrund Verbindungsdaten gespeichert werden, wie Zeitstempel, Betreffzeile, Adressat:innen oder IP-Adresse (=Internetprotokoll-Adresse, eine mehrstellige Nummer, die dem jeweiligen Gerät im Internet eindeutig zugeordnet ist, damit es überhaupt erreichbar ist). Administratior:innen können (z. B. über das Programm MS Defender [S. 74]) einsehen, wer wann welche Betreffzeile an wen versendet hat, was insbesondere dann erforderlich ist, wenn es zu technischen Problemen kommt. Diese Anzeigen für Administrator:innen gehören zum Standard und können technisch nicht abgeschaltet werden – sollen sie auch nicht, weil sonst keine Fehler entdeckt und behoben werden können.

Über den Exchange-Server [S. 73] können Regeln erstellt werden, wie mit E-Mails umgegangen werden soll, wie lange sie aufbewahrt werden, auf welcher Basis Spamfilter 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.

In Outlook gibt es die Einstellung „**Posteingang mit Relevanz**“. Ist sie aktiviert, werden „selbstlernend“, beispielsweise mittels dem KI-Programm Copilot [S. 62], „Prioritäten“ für E-Mails erstellt. MS ordnet, was für die Nutzer:innen wichtig ist – und was nicht. Anhand

der von Nutzer:innen markierten, gelesenen und beantworteten, also bewerteten E-Mails (z. B. wichtig / zur Nachverfolgung / erledigt) sowie hinterlegten organisationsinternen Hierarchien (z. B. Zuordnung zu Abteilungen, Leitungs- oder Assistenzposten) „lernt" Outlook, welche Absender:innen schnelle Antworten erfordern (z. B. die von Vorgesetzten), welche erst später Rückmeldung erfordern (das könnten möglicherweise wenig finanzkräftige Kund:innen sein) oder welche E-Mails aufgrund der Betreffzeile keinen Aufschub erlauben.

Outlook wohnt eine gewisse Verhaltenskontrolle inne.

**Zu E-Mails sollte in der BV geregelt werden:**

- Speicherdauer festlegen; welche E-Mails werden automatisch aufbewahrt? Welche E-Mails sind manuell aufzubewahren bzw. zu löschen?

- überbordende Kommunikation gilt es zu vermeiden, indem Benachrichtigungen aus Teams, Viva Insight und ähnlichen Tools über Statusänderungen [S. 51] möglichst eingeschränkt oder zumindest still gestellt sind.

- Vertretungsregelungen festlegen; Wer darf in das Postfach Einsicht nehmen, wenn jemand plötzlich abwesend ist? Vorgesetzte sollten nur in Notfällen die E-Mails der Arbeitnehmerinnen und Arbeitnehmer sehen oder an andere weiterleiten. Wer vertritt eine abwesende Kollegin oder einen abwesenden Kollegen, wenn E-Mails zu beantworten sind?

- Weiterleitungskonzept sowohl für geplante Abwesenheiten als auch für Notfälle;

Jede:r Arbeitnehmer:in erteilt einer Person ihres Vertrauens die Genehmigung bei ungeplanten plötzlichen Abwesenheiten (Krankheit, Pflegefreistellung) in ihr Postfach Einsicht zu nehmen, um dringend zu erledigende E-Mails an die sachliche zuständige Person weiterzuleiten.

ODER

Der Zugriff auf das persönliche Outlook-Postfach im Falle ungeplanter Abwesenheit erfolgt ausschließlich im Sechs-Augen-Prinzip mit einer Vertrauensperson des/der Abwesenden und der/dem betrieblichen Datenschutzbeauftragen sowie in Anwesenheit eines Mitglieds des Betriebsrates.

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

- Privatnutzung festlegen (z. B. eigenes Postfach)

- Stufenweise Kontrollverdichtung festlegen, für den Fall, dass Administratorinnen oder Administratoren Unregelmäßigkeiten oder Auffälligkeiten feststellen.

E-Mails werden grundsätzlich nicht automatisch weitergeleitet. Werden E-Mails aufgrund einer technischen Überprüfung als systemkritisch eingestuft, findet keine Übermittlung statt und die betroffenen Mails werden vorerst in einen gesonderten Ordner abgelegt und am Ende der darauffolgenden Woche endgültig gelöscht. Der/ die Empfänger:in kann sich über den Inhalt des Ordners jederzeit selbst informieren. Sollten von Seiten der Systemadministration Mailinhalte eingesehen werden, dürfen die dabei gewonnenen Erkenntnisse nicht zu Lasten der betroffenen Person verwendet werden. Sollten sich der/die Systemadministrator:in auf den Arbeitsplatz einer Mitarbeiterin oder eines Mitarbeiters aufschalten müssen, so ist dies nur für die Behebung technischer Probleme nach Zustimmung der Betroffenen möglich.

- Die Einsicht von Administrator:innen begrenzen auf das Vermeiden von Schad-Software, Angriffen, Datenverlust und Ähnlichen Sicherheitsrisiken.

Der **Kalender** dient dazu, die eigene Arbeit zu organisieren oder Termine gemeinsam abzuklären. Kalender sollten keine Arbeitsvorgaben enthalten. Kalender sagen im besten Fall etwas über das Zeitmanagement von Kolleg:innen aus und sollten folglich nicht zur Interpretation der Arbeitsleistung herangezogen werden, sollen nicht mit der Arbeitszeiterfassung automatisch verlinkt sein oder sonst wie im Zusammenhang mit der Arbeitszeiterfassung abgeglichen werden.

Über Exchange [S. 73] kann der Kalender – und dessen Statusanzeigen – für alle (freigeschalteten) Nutzer:innen einsehbar gemacht werden. Dabei sollte darauf geachtet werden, dass nur jene Kolleg:innen Einsicht in die Kalender haben oder diese bearbeiten dürfen, die das für ihre Arbeit tatsächlich benötigen.

Seit Oktober 2024 offeriert MS 365 eine neue Option. Wenn Nutzer:innen ihren **Standort** und ihre **Arbeitszeiten** freischalten, kann in Teams und damit auch über den Kalender von Outlook angezeigt werden, wer gerade im Büro ist und wer auf Telearbeit. MS verfasst dazu einen Hinweis: „Der Arbeitsstandort wird nicht zum Nachverfolgen von Mitarbeitern verwendet. Die Arbeitsstandortdaten von Personen werden aggregiert und anonymisiert, um die Trends der Bürobesetzung zu verstehen." Damit macht MS unmissverständlich klar, dass die Möglichkeit zur Standortüberwachung, nicht nur außerhalb des Arbeitsgebäudes, sondern auch innerhalb besteht. In einem Arbeitsumfeld mit flexiblen, je nach Tätigkeit wechselnden Arbeitsplätzen hätte dies eine gewisse Berechtigung. In anderen Settings hätte diese Funktion wenig Zweck und wäre daher zu deaktivieren.

Die Angabe, wer an welchem Ort die Arbeit erledigt, sollte nur für jene Kolleg:innen ersichtlich sein, die zum engeren Team zählen. Eine permanent und für alle Beschäftigten eines Unternehmens verfügbare Einsicht in Arbeitszeit und Arbeitsort wäre überschießend.

**Für Kalender können in einer BV folgende Punkte geregelt sein:**

- Zwecke festlegen; wird der Kalender für Aufgabenverteilung und -planung verwendet oder eine andere MS App (z. B. Teams [S. 43], Planner [S. 56], )?
- Einsicht regeln, wer wessen Kalender sehen oder wer Termine ein- und austragen kann, Lese- und Schreibberechtigungen möglichst eng begrenzen (z. B. auf die eigene Abteilung) oder von den einzelnen Benutzer:innen selbstbestimmt vergeben
- Standortangaben zur Telearbeit deaktivieren oder nur in einem eng begrenzten Bereich freischalten (z. B. eigene Abteilung)
- Auswertungsverbot von Outlook-Profilen oder eine konkrete Ausnahmeregelung bei anlassbezogenen, begründeten Verdachtsmomenten unter Beteiligung des Betriebsrats
- Automatisierte Benachrichtigungen anderer Apps deaktivieren (z. B. Vorschläge für Fokuszeiten oder „well-being" von Viva Insights standardmäßig deaktivieren)

## TEAMS

Teams kann wesentlich mehr als Videotelefonie. Teams zählt seit in den frühen 2020er Jahren zu den meisterweiterten Anwendung von MS. Bei Teams wurde sehr viel entwickelt, geforscht und Werbung betrieben. Teams ist mittlerweile zu einer eigenen Plattform ausgebaut, die für gemeinsames Bearbeiten und Ablegen von Dateien, das Versenden von Nachrichten, die Verknüpfung mit Terminen oder das Chatten (Plaudern) konstruiert ist. Teams ist für die Kommunikation und Zusammenarbeit – insbesondere seit dem vermehrten Arbeiten im Home-Office – ein viel genutztes Instrument. Gute Übertragungsqualität und vielfältige Funktionalitäten für vielfältige Medien wie Bild, Ton, Chats, Dokumente etc. ohne lästigen Wechsel von einem Format auf ein anderes sorgen dafür, dass MS Teams weit verbreitet ist.

Nachdem Teams immer umfassendere Einsatzmöglichkeiten erhalten hat, stand der Vorwurf seitens eines

Mitbewerbers (Slack) im Raum, MS würde den Wettbewerb im Europäischen Wirtschaftsraum bei Kommunikations- und Kooperationsprodukten einschränken. Die EU-Kommission wurde tätig und leitete im Sommer 2023 ein Verfahren wegen Wettbewerbsverzerrung ein, woraufhin MS kurzerhand Teams von den anderen MS-365-Angeboten entkoppelt hat. Die Plattform Teams ist nun als eigenes Produkt erhältlich und muss nicht mehr im Paket mit anderen MS-Diensten genutzt werden.

Wird Teams im Unternehmen als Teil des MS 365 Gesamtpakets genutzt, sind im Hintergrund Informationen aus dem Active Directory [S. 78] verknüpft, Es besteht eine Verknüpfung zum Exchange-Server [S. 73], bzw. dem E-Mail-Postfach und dem Kalender [S. 41] sowie zu SharePoint [S. 67]. Auf der Plattform Teams können wiederum weitere Anwendungen von MS 365 eingehängt werden – soweit sie für die oder den jeweilige:n Nutzer:in freigegeben sind. Auf Teams können folglich Arbeitsschritte miteinander verbunden werden und sind dort auch ersichtlich (z. B. E-Mails, Kalender, Präsenzstatus, Aktivitäten in Dateien u.s.w.).

Administrator:innen mit der entsprechenden Berechtigung können im „User-Activity-Report" sehen welche Teams wie viele Chats, Calls, Meetings, Uploads, Downloads u.s.w. gemacht haben.

Werden Zugriffe auf SharePoint, Teams oder OneDrive unterschiedlich eingerichtet, wird es schnell unübersichtlich. Nutzer:innen sind verwirrt von nicht mehr auffindbaren Dateien, Dateien ohne Zuordnung, auf SharePoint vorhandenen obwohl eigentlich gelöschten Unterlagen etc. Um Verwirrungen zu vermeiden, muss sorgfältig darauf geachtet werden, wer welche Berechtigungen hat und für welche Zwecke Teams verwendet wird.

Auf Teams können weitere Untergruppen eingerichtet werden, so genannte **Channels** (z. B. für Projekte innerhalb eines Bereichs).

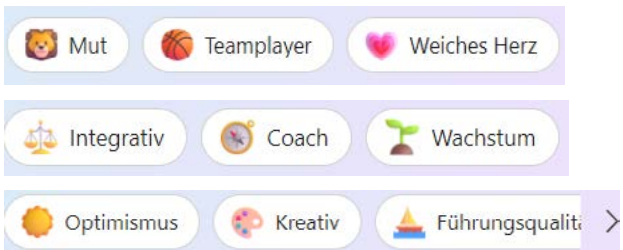
In Teams ist eine gern genutzte **Chat**-Funktion enthalten, mit der die Teilnehmenden entweder eins zu eins oder für alle lesbare Nachrichten austauschen können. Individuelles Löschen der Chats ist seit Jänner 2023 möglich, wobei nur die Ansicht gelöscht wird, der Chat selbst erhalten bleibt.

Die **Übersetzung** von Sprache in Text (Untertitel) sowie in andere Sprachen wird – zumindest für häufig gesprochene und geschriebene – immer besser und ist vor allem für internationale Treffen hilfreich (z. B. bei einem Europäischen Betriebsrat). Untertitel sind (derzeit) in Englisch, Chinesisch, Niederländisch, Französisch, Deutsch, Hindi, Italienisch, Japanisch, Koreanisch, Portugiesisch, Russisch, Spanisch und Schwedisch verfügbar. Falls die Übersetzung der Redebeiträge protokolliert und aufbewahrt werden soll, ist eine Überarbeitung dringend empfohlen. Außerdem sind natürlich alle Beteiligten darüber zu informieren, die Zwecke klarzustellen (z. B. Protokollierung einer Sitzung und keine Weitergabe an Dritte) sowie eine Aufbewahrungsdauer zu fixieren.

Die mittlerweile sehr fortgeschrittene **Sprachassistenz** steht bei Teams in Kombination mit dem Copilot [S. 62] zur Verfügung, um Texte vorzulesen oder Sprache in Text umzuwandeln. Die Assistenz kann eingesetzt werden um zu diktieren oder auch um Befehle auszuführen wie „Suche einen Kalendereintrag mit Kollege xy".

Über Teams können Spielereien wie Gifs (das „Graphics Interchange Format" steht für kleine bewegte Bilder, die wenig Speicherplatz benötigen), Memes (das sind kleine, einfache, meist lustige Bilder, die im Internet verbreitet werden) oder andere Inhalte versendet werden (man nennt diese Anlehnung an die Welt der Spiele auch „Gamification"). Mittels „**Praise**" (engl.: Lob) kann man **Bewertungen** an Kolleg:innen verschicken.

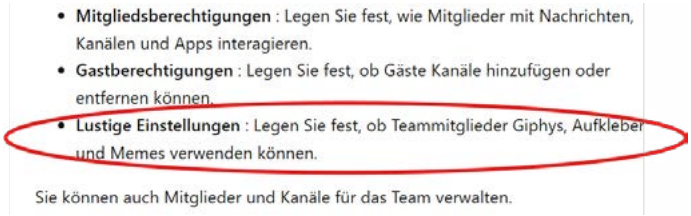
MS 365 bietet dieses „Lob" in Form von kleinen Bildchen mit Löwen (der Mutige), einer Faust (der Problemlöser), einem Pokal (Gratulation), einem Basketball (Teamplayer), einer Sonne (Optimismus), einem Blumentopf (Wachstum) und weiteren Symbolen an. Die Bilder könnten als Bewertung der Arbeitstätigkeit, als Feedback oder auch als „leise" Kritik gesehen werden.



Es wird getrackt, wer wem was wann wie oft schickt (wobei MS beteuert, dass die Darstellung ausschließlich den Empfänger:innen selbst zur Verfügung steht). Jede:r Nutzer:in kann sich ansehen, welches „Lob" er oder sie von wem im Laufe der letzten Zeit erhalten hat. Mit der entsprechenden Berechtigung können auch Vorgesetzte die „Praise-History" der Beschäftigten ansehen. Dass dadurch schnell Fehlinterpretationen entstehen können, liegt auf der Hand. Ein spaßeshalber zugesendetes Segelboot könnte ebenso eine Erinnerung an den letzten Urlaub sein, wie die von MS zugeschriebene Charaktereigenschaft „Führungsqualitäten".

Ob diese Elemente der Gamification im Arbeitsalltag motivieren, ablenken oder demotivieren, ob sie benötigt werden oder nicht, ist abhängig von der Betriebskultur bzw. Geschmackssache. Der Interpretationsspielraum derartiger Bewertungen ist sehr breit. Die Verwendung der Bildchen kommt dem Spieltrieb entgegen, fördert die Interaktion untereinander und schnell vergeht die Zeit...

Die Praise-Funktion kann über das Admin-Portal, also von dazu berechtigten Administrator:innen, ausgeschalten werden.




In einer Betriebsvereinbarung wurde der Umgang mit den Bildchen folgendermaßen festgelegt:

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

Lob, auf Englisch „Praise", kann auch über die App Viva Insights [S. 52] versendet werden, weshalb alles oben Dargelegte für Insight ebenso gilt.

Grundsätzlich geht man auf der Teams-Plattform davon aus, dass alle gleichberechtigt darin arbeiten und alle alles sehen. Sollten hingegen bestimmte Kollaborationsräume und die darin ausgetauschten Informationen nur bestimmten Personengruppen zur Verfügung stehen, werden Untergruppen („Channels") eingerichtet. Je mehr verschiedene Teams, je mehr Channels, je mehr unterschiedliche Leseberechtigungen einem User oder einer Userin zugeordnet sind, desto komplizierter wird es und Teams funktioniert nicht mehr ganz so effektiv. Wer darf oder soll in welcher Untergruppe welche Informationen bereitstellen? Hier eine gut funktionierende Balance herzustellen zwischen Datenintegrität und -stabilität bei gleichzeitiger Aktualität und Richtigsstellungsmöglichkeit, zwischen einfacher Übersichtlichkeit und Komplexität, zwischen Vertraulichkeit und Transparenz ist eine der größten Herausforderungen bei der Plattform.

Ein internationaler Konzern hat den Umgang mit den Untergruppen bei Teams in einer BV wie folgt festgelegt.

> Nur die zuständigen Mitarbeiter der IT-Abteilungen legen Teams und Channel an und sind deren Besitzer. Besitzer können auf begründete Anforderung Beiträge löschen.

Ganz ohne Hierarchien geht es auf Teams nicht. Vortragende erhalten eigene Berechtigungen („special skills") um Teilnehmer:innen-Berechtigungen zu moderieren (z. B. Bildübertragung wird allen Teilnehmenden bei großen Zusammenkünften entzogen, um die Übertragungsqualität zu erhalten). „**Besitzer**" nennt MS diejenigen, die die Berechtigung haben, ein Team zu erstellen, also in der Regel Leiter:innen eines Bereichs, einer Gruppe, einer Abteilung, einer Filiale.

MS 365 übermittelt **Telemetriedaten** (Diagnosedaten wie z. B. letzte Softwareupdates, Fehlerdokumentation, Anwendungsdauer, Nutzungshäufigkeit, Verbindungsunterbrechungen, Geschwindigkeit der Übermittlung,

Datenschutzeinstellungen etc.) an Microsoft. Dies sollte durch technische Voreinstellung deaktiviert bzw. eingeschränkt werden.

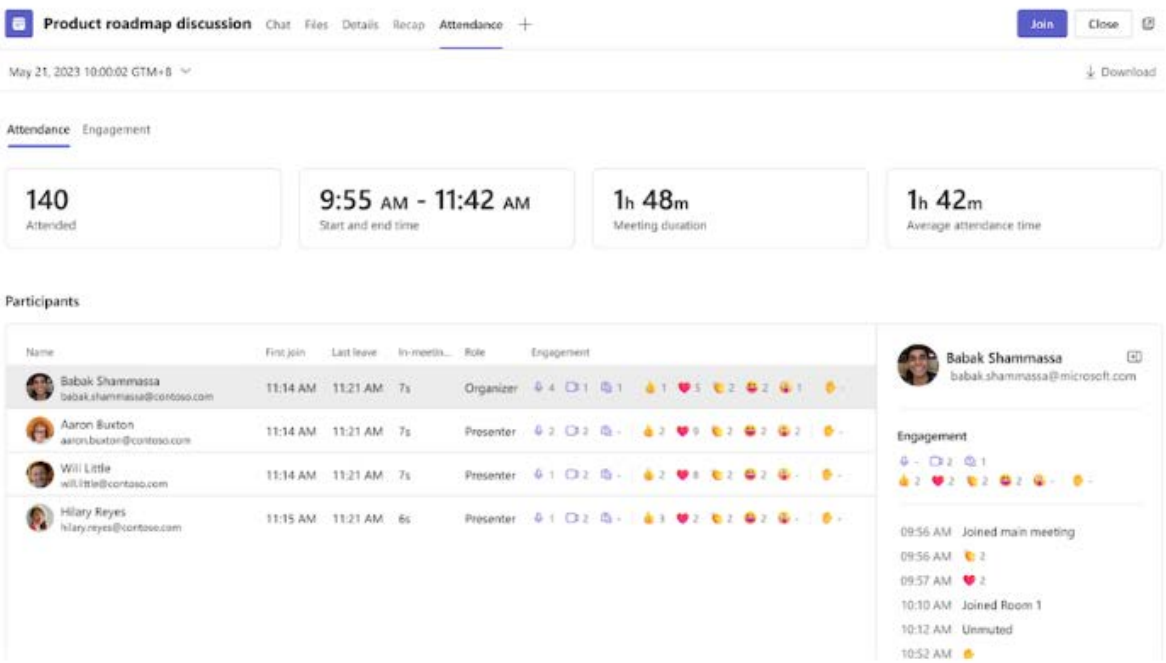
Die Tätigkeiten der letzten sieben bis 28 Tage können mit dem (2020 neu zur Verfügung gestellten) **Analysetool** für die „Besitzern/Owner", ausgewertet werden. Seit 2020 steht für Teams-Owner ein Excel-Sheet zur Verfügung auf dem nachverfolgbar ist, wer wie lange an einem Meeting teilgenommen hat, wer das Meeting für wie lange verlassen hat oder wer zu spät gekommen ist. Der Zeitstempel auf der Teilnehmer:innen-Liste verrät: Wie oft tauschen sich die Gruppenmitglieder aus, wie „aktiv" ist die Gruppe? Welche Features wurden genutzt? Wie viele Megabyte wurden hochgeladen? In seinem im Oktober 2022 veröffentlichten „Datenschutzreport" gibt MS Auskunft, welche Diagnosen/Analysen in Teams durchgeführt werden. Gruppenleiter:innen/ Besitzer:innen können sich über den „Benutzeraktivitätsbericht" anzeigen lassen, wer wie viele Sitzungen organisiert, wer an wie vielen Sitzungen teilnimmt, mit wem viel oder wenig „Kontakt" hat.

**Anonymität** ist in Teams also nur bedingt gegeben. Je kleiner die Gruppe auf Teams oder im Channel, desto weniger Anonymität. Daher wird es Schulungen, Bewusstseinsarbeit, und Betriebsvereinbarungen brauchen, damit diese Daten nicht zu unlauteren Zwecken eingesehen und verwendet werden und schon gar nicht zu nachteiligen Interpretationen für die Beschäftigten führen.

Das Ein- und Ausschalten der Funktionen bei Videotelefonaten, **Videocalls**, sollte so weit als möglich freiwillig erfolgen. Kamera, Mikrofon- und Freigabe von Dokumenten sollten von den Teilnehmer:innen selbstständig aktiviert und deaktiviert werden.
Teams bietet bei der Verwendung der **Kamera** eine Funktion, die den Hintergrund unscharf erscheinen lässt. Diese sollte von den Nutzer:innen besonders dann eingeschalten werden, wenn sich andere Personen im Raum befinden (z. B. Mehr-Personen-Büros, Home-Office). Sollten weitere Personen ins Blickfeld der Kamera geraten können, müssen diese darüber informiert werden.

### ENGAGEMENT IM TEAM!?

Organisatoren mit Teams Premium können Nach einer geplanten Besprechung oder einem Webinar Auf der Registerkarte **Anwesenheitsdaten** wie Gesamtreaktionen, erhobene Hände, aktivierte Kameras und vieles mehr anzeigen und herunterladen.



**Audio- und Videoinhalte** können in MS Teams **gespeichert** werden. Ein solcher Mitschnitt bedarf aber der vorherigen Information und ausdrücklichen Zustimmung der Teilnehmer:innen. Eine Aufzeichnung von Konferenzen/Gesprächen/Webinaren kann für die spätere Nachvollziehbarkeit mitunter Sinn machen (z. B. Reklamation bei Dienstleistungen, Entscheidungsfindungen von Gremien), sollte allerdings auf einen engen Zweck beschränkt werden (z. B. konkrete Schadensersatzansprüche, Ergebnisse festhalten).

Ein Betrieb hat die Verwendung von Mikrophon und Kamera wie folgt geregelt:

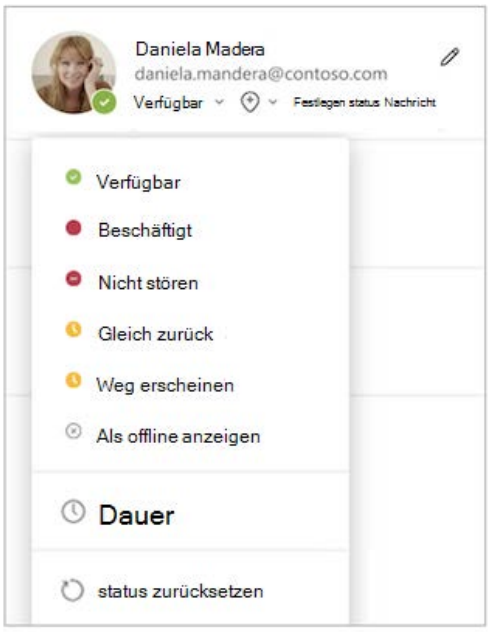
> Audio- und Videoinhalte können nach vorheriger Information und ausdrücklicher Zustimmung der Teilnehmer:innen der Konferenz durch den/die Organisator:in aufgezeichnet werden. Die Aufzeichnung wird jedem/r Teilnehmer:in auf dem Bildschirm signalisiert. Eine Aufzeichnung sowie deren Weitergabe oder Bekanntmachung an Dritte außerhalb der teilnehmenden Personen, bedarf der vorherigen ausdrücklichen Zustimmung sämtlicher Gesprächspartner:innen. Falls eine Freisprechfunktion genutzt wird, ist der/die 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 Chat-Verläufe zu verstehen. Abgesehen von der Aufzeichnung von Webinarinhalten sind Weisungen zu einer verpflichtenden Audio- oder Videoaufnahme unzulässig.

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

Mit der MS **Teams Rooms Pro** Lizenz und einer bestimmten Kategorie von Kameras ist es möglich, für bis zu maximal 12 Personen im Teams-Raum und maximal 64 Besprechungsteilnehmer:innen insgesamt „intelligente Kameras" zu verwenden, die mit KI zur Gesichts- und Spracherkennung ausgestattet sind. Dieses Feature heißt „**IntelliFrame**". Es verwendet biometrische Merkmale, um den Teilnehmenden, die gerade sprechen, das richtige Profil zu zuordnen. Es wird auf die sprechende Person gezoomt. Ob dieses Feature gebraucht wird, ob der Zweck mit einem gelinderen Mittel erreicht werden kann, ob also der „Zweck die Mittel heiligt", 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.

Teams bietet ein „**Sofortprotokoll**". Besprechungsnotizen können hier für alle Teilnehmenden innerhalb des Unternehmens, nicht aber für Teilnehmende von außerhalb, transparent gemacht und (bei entsprechender Freigabe) gemeinsam bearbeitet werden.

MS Teams zeigt den „**Status**" an, ob Kolleg:innen gerade „in einer Besprechung" oder „in einem Call" sind, was aufgrund des Terminkalenders [S. 41] oder der aktiven Telefonfunktion festgestellt wird.




Der Status kann nicht nur in Teams sondern auch in Outlook [S. 41] und Sharepoint [S. 67] angezeigt werden. Um einen der Realität entsprechenden Informationsstand über den Status der Beschäftigten zu erhalten, müssten diese den Status jeweils in Echtzeit korrekt

angeben, Termine im Kalender akkurat einhalten, ihre Telefonate über MS Phone führen. Es fragt sich, ob permanente Statusanzeigen im Arbeitsalltag hilfreich sind (siehe Interpretation von Beschäftigten-Daten [S. 11]) oder ob dies zu einem ausgeprägten Rechtfertigungsdruck führt, warum jemand gerade „nicht verfügbar" ist oder zu der Erwartung stets über den „Status" der Kolleg:innen Bescheid zu wissen.

Seit 2024 kann auch der **Arbeitsort** in Teams angegeben werden mit der Möglichkeit „im Büro" oder „remote" auszuwählen. Je nach Wunsch können unterschiedliche Gebäudestandorte, Büros, Filialen im Unternehmen hinzugefügt werden. Das könnte natürlich zu einer enggliedrigen Überwachung der Beschäftigten führen.

Soll der Arbeitsort sowie der Präsenzstatus in Teams generell deaktiviert werden, braucht es eine:n Administrator:in. Diese können im „Employee Center" die jeweiligen Profile über die Option „Show MS Teams Presence" so abändern, sodass entweder die Anzeige „permanent offline" bleibt oder der „Privacy Mode" aktiviert ist sodass Nutzer:innen selbst bestimmen können, welcher Status für welche Dauer an Kolleg:innen angezeigt wird.

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

Teams versendet – so diese Einstellung vorgenommen wurde – eine **Benachrichtigung** (z. B. in Form eines E-Mails), wenn eine Aktivität im Team stattfindet. Möchte man nicht bei jeder kleinen Änderung in einem Channel, bei einer Aktivität, bei einer Dateiänderung, bei neuen Teammitgliedern und Ähnlichem, ein automatisiertes E-Mail ins Postfach bekommen, sollte man diese Benachrichtigungen deaktivieren.

In Teams können über das Admincenter – so die Berechtigung dafür vorhanden ist – weitere beliebige Apps aus der Welt außerhalb von MS 365 eingebunden werden.

Seit Jänner 2024 soll **Copilot** [S. 62] Meetings in Teams „intelligenter, personalisierter und geschützter machen", schreibt MS, indem beispielsweise empfohlen wird, was als nächstes zu tun wäre, Inhalte von Dateien zusammengefasst werden, Protokolle von Sitzungen erstellt oder englischsprechende Meeting-Teilnehmende in Echtzeit, also simultan, übersetzt werden.

Die zahlreichen Verknüpfungen und Funktionalitäten von Teams lassen bei den Nutzer:innen ein bisweilen verwirrendes „Erlebnis" zurück. Es sollte daher eindeutig in einer BV dargelegt werden, wofür Teams verwendet wird und wozu es andere Kommunikationskanäle gibt (z. B. das jährliche Mitarbeiter:innengespräch). Es sollte klar geregelt sein, wer worauf Zugriff hat.

**Gute Voraussetzungen für gute Nutzung von Teams:**

- an die aktuellen Arbeitsaufgaben angepasstes Berechtigungsmanagement (sonst haben die Beschäftigten veraltete oder fehlende Zugriffsberechtigungen)
- strukturiertes Dokumentenmanagement inklusive Archivierung (sonst wird es unübersichtlich welche Dateien die aktuellen bzw. die richtigen sind und wo sie liegen)
- klare Einteilung der Teams und Channels (sonst kommt es zu Doppelungen)
- eindeutiges Meeting-Management (sonst werden zu viele Termine / Meetings / Anfragen gestellt und die Erwartungshaltung an ständige Erreichbarkeit wird überbordend)
- Filtern oder Deaktivieren der Benachrichtigungen innerhalb der verschiedenen Teams, Channels, Chats und Outlook (sonst kommt es zu einer Flut an Benachrichtigungen auf sämtlichen Apps)




- Zuständigkeiten klären (sonst ist es kaum möglich, verpflichtende von freiwilligen Aktivitäten zu trennen)
- Schulungen (sonst erkennen Nutzer:innen den Zweck nicht, nutzen Teams nicht zweckentsprechend und es fehlt an Akzeptanz)
- Datenschutz und Compliance (sonst entstehen (Sicherheits-)Lücken wodurch Transparenz und Vertraulichkeit verloren gehen)
- Schnittstellen-Management (sonst können beliebig viele Apps eingebunden werden, was zu Verwirrung führt)

Eine Betriebsvereinbarung ist der ideale Ort für die gemeinsame Festlegung des betriebsinternen Umgangs mit Teams. Um den Umgang mit Teams zu schulen und zu üben, holen sich Unternehmen mitunter eigene spezialisierte **externe Berater:innen** an Bord. Der Betriebsrat sollte sich in der BV zusichern, 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 Privatsphäreschutz spezialisiert ist.

**Für Videokonferenzen via Teams sind Regelungen in einer Betriebsvereinbarung zu treffen:**

- Zweckbestimmung (z. B. interne Informationsveranstaltung, externe Weiterbildung etc.)
- Rollenkonzept und Zugriffskonzept (wer darf Teams leiten, Teilnehmer:innen stumm schalten; wer darf teilnehmen, einladen? Wer darf Aufnahmen, Chats downloaden oder speichern?)
- Rechte am eigenen Bild/Text vorab klären; Informationen aller Teilnehmenden zu allfälligen Ton- und Bildaufzeichnungen inkl. Widerspruchsrecht

- Gesichtserkennung als Standardeinstellung deaktiviert (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)

- Administrator:innen-Rechte so einschränken, dass diese keine Aufnahmen machen können oder nur für eingeschränkte Zwecke (z. B. Schulung, Protokollierung, Transkripterstellung etc.).

- Den Umgang mit allfälligen Aufzeichnungen regeln (für wen wird das Recording zur Verfügung gestellt? Wo wird es gespeichert? Wann wird es gelöscht? Wann darf transkribiert werden? Muss diese Mitschrift/Protokoll überarbeitet und freigegeben werden?)

- Freiwilligkeit von Ton- und Bildaufnahmen sowie enge Zweckbindung (z. B. Schulungen)

- empfohlene Standardeinstellung falls im Privatbereich oder mit anderen Personen im Raum eine Konferenz stattfindet: Hintergrund verschwimmend oder ein vorgegebener Hintergrund

- Verwendung eines Headsets/Kopfhörer vereinbaren, insbesondere wenn weitere Personen im Raum sind

- Sind die Konferenzen länger als eine Stunde, sind Pausenregelungen zu treffen (Bildschirmpause)

Das Aktivieren der Aufnahme-Funktionen 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. Der/die Teilnehmer:in ist verpflichtet, im Raum anwesende Personen über die aktivierte Kamerafunktion zu informieren. Weisungen zur Verwendung des Live-Bildes sind unzulässig.

**Für die Betriebsvereinbarung zu Teams als App für die Zusammenarbeit sind folgende Regelungen zu überlegen:**

- Zweck angeben (z. B. gemeinsame Dateienbearbeitung innerhalb einer Projektgruppe)

- Festlegen, wann nicht mehr genutzte Teams oder Channels (samt allfällig angelegten Dateien/ Bibliotheken/ Kanälen/ Arbeitsräumen/ Protokollen/ Videos etc.) nach Projektende wieder gelöscht werden.

- Ausführliche Schulung als Vorbedingung verankern, die jedenfalls die möglichen Privacy-Einstellungen beinhaltet; insbesondere für „Teams-Owner", also jene, die Teams und Channels erstellen

- Berechtigungen festlegen, wer welche Aufgaben in Teams hat. Festlegen, wer die Leitung inne hat und 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 Bearbeitungsprotokolle/Teilnehmer:innen-Listen u.s.w. keine Beurteilung von und kein Vergleich zwischen Kolleg:innen erfolgen darf

- Festlegen, wofür Chats verwendet werden (falls sie nur zum Plaudern dienen, festlegen, dass sie automatisch mit Ende der Sitzung gelöscht werden)

- Praise/Giphy/Memes etc. deaktivieren oder jegliche Auswertungen unterbinden

- Bei der gemeinsamen Dokumentenbearbeitung sollte der Befehl „Steuerung anfordern" nicht freigegeben werden. Damit hätte die/der anfordernde Nutzer:in die Möglichkeit, sich als die jeweils andere Person auszugeben und in deren Namen Dokumente zu ändern oder zu löschen.

- Freiwilligkeit von Statusanzeigen; keine Auswertung der vorhandenen Statusanzeigen

Der Präsenzstatus, das ist die Information darüber, ob Kolleg:innen gerade erreichbar, außer Haus oder beschäftigt sind, lässt sich dauerhaft auf „offline" stellen. Diese Möglichkeit sollte im Admincenter freigegeben werden, damit permanente Erreichbarkeit weniger zur (unausgesprochenen) Zielvorgabe wird.

- Umgang mit un-/gelesenen Nachrichten; soll die IT-Administration die Anzeige bei den Datenschutzeinstellungen deaktivieren; die Auswertung wer wessen Nachrichten/Dokumente/ Chats wie schnell liest/ antwortet deaktivieren?

- Löschregelungen festlegen; sowohl für Chats als auch für Channels, Unterhaltungen, Dokumente etc.; die Standardeinstellung „alles speichern" deaktivieren

Für das gemeinsame Arbeiten an Dokumenten, können die Teilnehmer:innen ihren Desktop frei geben, so dass andere diesen sehen können. Die Freigabe des Desktops muss explizit von dem/der Teilnehmer:in initiiert und bestätigt werden. „Verdeckte" Aktionen von anderen Teilnehmer:innen sind nicht möglich.

- Der Teilnehmer:innenkreis bei einer Dokumentenfreigabe sollte zu jedem Zeitpunkt für jede:n Teilnehmer:in ersichtlich sein.

## STATUS

Hierbei handelt es sich nicht um eine eigene App sondern um eine Funktion, ein Feature, das in einigen Anwendungen von MS 365 beinhaltet ist (z. B. Outlook [S. 41], Teams [S. 43]). Über die Anzeige des Status können andere Nutzer:innen erkennen, ob jemand gerade erreichbar ist oder warum jemand nicht erreichbar ist (z. B. Urlaub).

Diese Information ist nicht nur für die Kolleg:innen ersichtlich, sondern auch MS verwendet sie weiter, stellt damit Berechnungen an und gibt – falls Viva verwendet wird – in Viva Insights [S. 52] Tipps, wie die Zeiteinteilung optimiert werden könnte.

Der Status wird automatisch über den Terminkalender bestimmt.

Der Benutzer kann jederzeit seinen Status frei wählen (verfügbar, abwesend). Dabei ist der Status so zu konfigurieren, dass nur der momentane Status angezeigt wird, aber nicht die vergangenen Status. Es ist allen Anwendern jederzeit freigestellt, den Status nach eigenem Ermessen zu setzen.

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

- Deaktivierung der Möglichkeit, andere Nutzer:innen über Statusänderungen zu benachrichtigen

- Auswertungsverbot für Analysen, deren Zweck es ist individuelles Verhalten zu vergleichen oder zu beurteilen

Die Funktion „Benachrichtigen wenn verfügbar" ist problematisch. Dabei wird eine Nachricht an die Person, die dies anfordert, versendet, sobald die/der gewünschte Kollegin/Kollege den Status „verfügbar" hat – mit dem Schönheitsfehler, dass die gewünschte Person nichts davon weiß und diese Benachrichtigung, selbst wenn sie es wollte, nicht unterbinden kann. Eine Nachricht „Bitte ruf mich zurück" wäre vermutlich ausreichend und würde die gewünschte Person nicht einer heimlichen Statusüberwachung aussetzen. Von der Funktion „Benachrichtigung wenn verfügbar" sollte daher Abstand genommen werden.

**In der BV zu MS 365 sollte geregelt werden:**

- möglichst wenige Status verwenden (z. B. „frei“ und „beschäftigt“ ist in der Regel ausreichend)
- Status als Arbeitszeiterfassungsinstrument untersagen

Damit aus Statusanzeigen keine falschen Interpretationen abgeleitet werden, haben einige Betriebe das geregelt.

> 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.

## VIVA

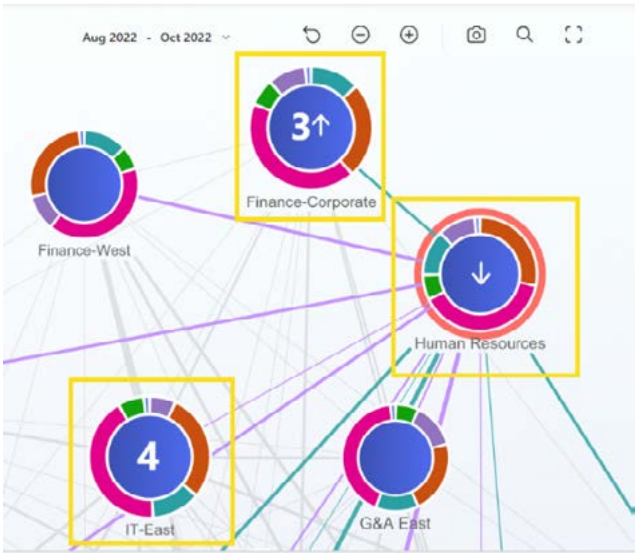
Viva besteht aus verschiedenen Anwendungen (Insights, Learning, Engage, Glint, Connections, Sales, Suite, Topics, Amplify, Pulse, und Workplace Analytics), die teilweise im allgemeinen MS365-Paket mit dabei sind oder zugekauft werden können. Viva liefert vorwiegend Austauschplattformen und (persönliche) Analysen.

### VIVA Insights

Ein Vorgänger-Modell von Viva Insights mit ähnlichen Analysefunktionen brachte Microsoft kam erstmals 2015 unter dem Namen „Delve Organisational Analytics“ auf den Markt. Damit konnten sich Nutzer:innen ihre favorisierten Kommunikationspartner:innen, ihre wichtigsten Dateien, ihre wesentlichen Aufgabengebiete darstellen lassen. 2017 wurde dieses Feature auf eine ganze Gruppe ausgedehnt und unter dem Namen „Workplace Analytics“, bzw. „My Analytics“ in der individuellen Variante, eingeführt – und in der Fachwelt als äußerst datenschutzkritisch wahrgenommen. Die App berechnete unter anderem einen so genannten „Produktivitätsscore“ für jede:n Nutzer:in oder gab persönliche Tipps zur Work-Life-Balance. Die eher diffusen Auswertungen sorgten für Diskussionsstoff. Ein weiteres Problem bei Viva Insights war dessen Datenübermittlung in die USA. Dieses Transferproblem hat Microsoft behoben, indem die Daten 2022 in ein europäisches Rechenzentrum verlagert wurden.
Seit 2021 bedient die App namens Viva Insights ähnliche Zwecke.

Wer das Feature Viva Insights verwendet, erhält Tipps zur „Reflexion“ (um Zeit zu reservieren), für „Effiziente Besprechungen“ (um Teams-Meetings nicht für länger als eine Stunde anzusetzen), für „virtuelles Pendeln“ (um an das Ende der Arbeitszeit erinnert zu werden), für „Zeitfenster blockieren“ (um ungestört von Benachrichtigungen arbeiten zu können), „Lob“ (um motivierendes Feedback in Form von Bildern zu versenden)

**NETZWERKANALYSE IM UNTERNEHMEN: WO ENTSTEHEN „INSELN“?**



und Ähnliches. Der/die Nutzer:in erhält regelmäßig, auf das persönliche Verhalten abgestimmte Vorschläge (z. B. wem man ein Lob senden sollte oder wann Zeit zur Reflexion wäre). Ein Betriebsrat erzählt, dass die Funktion „Zeitfenster blockieren" gerne von den Kolleg:innen genutzt wird, um so im Outlook-Kalender für die anderen blockiert zu sein und in Ruhe arbeiten zu können.

Viva kann die Beziehung zwischen einzelnen Beschäftigten, Abteilungen mit unterschiedlich dicken Linien darstellen und nach Kommunikationswegen (z. B. E-Mail, Chat, Meeting) filtern. So könnte eine Darstellung ergeben, dass Team A mit Team B insgesamt eng kooperiert, sich aber noch nie persönlich getroffen hat. Eine Empfehlung daraus könnte lauten: „organisieren sie ein Präsenz-Meeting zwischen Team A und Team B". Problematisch wird es, wenn Viva Insights von Unternehmensseite für ein sogenanntes „Organizational Network Analysis, ONA" eingesetzt wird (das ist eine Netzwerkvisualisierung, wie in der Grafik [S. 52]), mit dem gezeigt wird, wer mit wem am meisten zusammenarbeitet, Wissensflüsse, Schlüsselpersonen und (entstehende) Isolation von Abteilungen untersucht werden.

Solche Analysen beruhen auf Daten aus Outlook, Teams und anderen Apps. Sie sind mit Vorsicht zu genießen, da sie ausschließlich Daten aus der MS-Welt enthalten, (schwierige) Rahmenbedingungen außen vor lassen, rein auf mathematischen Berechnungen beruhen und schlussendlich zu (falschen) Interpretationen verleiten.

Eine solche Netzwerkanalyse zeigt nicht, ob und wie intensiv sich Personen direkt, von Angesicht zu Angesicht austauschen bzw. wie das ihre Produktivität oder Kreativität oder den sozialen Zusammenhalt beeinflusst. Es wäre also nicht nur datenschutzrechtlich und arbeitsrechtlich unzulässig daraus Konsequenzen abzuleiten, sondern widerspricht auch dem, was Microsoft seinen Kund:innen vermittelt – effektive, kreative und engagierte Mitarbeiter:innen. Die dargestellten Netzwerke bilden nur ein Bruchteil, der sozialen und organisatorischen Beziehungen in einem Unternehmen ab – also höchstens einen Einblick aber keinen Rund-um-Blick.

Die Funktion „Besprechungsgewohnheiten" der Registerkarte Produktivität von Viva Insights zeigt, wie oft man Besprechungen organisiert, wie oft man zu online-Besprechungen eingeladen ist und an ihnen teilnimmt, ob man pünktlich ist, unter einer Stunde fertig ist etc. Wenn es keine gute rechtliche Begründung dafür gibt, dass Vorgesetzte oder Kolleg:innen diese Analyse sehen, sollte sie – insbesondere für Vorgesetzte – nicht aktiviert werden.

Viva Insights ist nur für den/die jeweilige Beschäftige:n einsehbar und die Analysemöglichkeiten für Gruppen bzw. Teams sind deaktiviert.

Die Funktion „persönliche Einblicke" in Viva Insights sollte ausschließlich freiwillig aktiviert werden.

Über die KIs Copilot [S. 62] sowie Analytics können in Viva Engage die Stimmung im Unternehmen (unterteilt in positiv, negativ und neutral) sowie die Netzwerke, also die Verbindungen innerhalb der Kollegenschaft, analysiert werden (z. B. mit wem oder welcher Beschäftigtengruppe hat die Betriebsrätin besonders häufig Kontakt in Chats, Mails, Termine). Zwar wird bei der Darstellung der Ergebnisse auf Anonymität geachtet, indem Gruppen unter 20 Personen bzw. 5 % nicht ausgewiesen werden, so MS, doch werden gleichzeitig offensichtlich Inhalte von Kommunikationen zusammengefasst und Emotionsanalysen erstellt.

Viva bietet Module, die weniger „neugierig" sind, wie **Viva Learning**, wo Lerninhalte aus dem gesamten Unternehmen oder auch externe Angebote für die Kolleg:innen bereitgestellt und empfohlen werden. Die Angebote auf der Plattform können - mitunter mit einer KI – an das individuelle Arbeitsprofil angepasst werden.

**Viva Connections** ist als eine Art personalisiertes „Schwarzes Brett" für die wichtigsten Informationen eines Unternehmens konzipiert.
Ein Betriebsrat berichtet, dass diese App für den gesamten Konzern zur freiwilligen Verwendung bereitgestellt wurde, was zu einer unübersichtlichen Fülle an Beiträgen führte. Zahlreiche Kolleg:innen wollten sich und ihre Arbeit über die App präsentieren. Die Geschäftsführung reagierte mit einer Handlungsanweisung:

> Bitte verwenden Sie Viva Connections nur für allgemein relevante Informationen die für alle Mitarbeiter:innen interessant sein können.

**Viva Engage** (vormals Yammer) ist als Austauschmedium gedacht, wo sich Kolleg:innen persönlich einbringen können. Die App kann als betriebsinterne Social-Media-Plattform genutzt werden, in der, wer möchte, Notizen, Bilder, Ideen und Vieles mehr hinterlässt.
Im Jänner 2025 erhielt diese App ein neues Feature für Netzwerk-Administrator:innen oder „besondere Berechtigte", mit dem Schlüsselwörter analysiert werden können. In der „Roadmap" [S. 34] schreibt MS: „Netzwerk und verifizierte Administratoren können bestimmte Schlüsselwörter einrichten, um Gespräche in ihren Netzwerken zu überwachen." In einem neuen Dashboard wird dies den Berechtigten angezeigt.

> Der Betriebsrat sollte derartige Schlüsselwort-Analysen unterbinden und sich zur Kontrolle das Dashboard der dazu berechtigten Nutzer:innen ansehen können.

**Viva Glint** ist nicht im Standard-Lizenzmodell von MS 365 enthalten (Stand Ende 2024), also extra bezahlt werden. Es dient Vorgesetzten, um sich über die „Stimmung und das Verhalten" im Team zu informieren, indem beispielsweise kurze Fragen versendet werden oder die Aktivitäten der Teammitglieder in verschiedenen Anwendungen von MS 365 angezeigt werden.

Viva greift unter anderem auf Daten aus Outlook [S. 41] zu, möglicherweise um auf Basis der Betreffzeilen in E-Mail herauszufinden, welche Themen wichtig sind und daraus ein individuelles Lernangebot zusammenzustellen.
MS selbst macht seine Kund:innen darauf aufmerksam: „Tipp: Kunden sollten die minimalen und am wenigsten vertraulichen Daten hochladen, die zum Erreichen ihrer Ziele erforderlich sind. Es liegt in der Verantwortung des Kunden, seine Datenschutz- und Complianceverpflichtungen zu bewerten und zu bestimmen, ob Glint geeignet ist. (....) Es wird erwartet, dass die Benutzer über Schulungen im Umgang mit vertraulichen Informationen verfügen."[8]

Viva lernt mit, wer welche Vorlieben hat und entwickelt daraus Tipps. Man könnte sagen, Viva ist „Privatdetektiv:in" innerhalb der MS Apps und findet heraus, wer was weiß und wer sich wann wozu mit wem und wo austauscht. Aus Netzwerkanalysen, zunehmenden außerbetrieblichen und abnehmenden innerbetrieblichen Kommunkationspartner:innen, aus herausgefilterten Stichwörtern oder weniger Teilnahme an (internen) Meetings könnten etwa (unzutreffende) Kündigungswahrscheinlichkeiten abgeleitet werden. Ein Schelm, wer meint, die weitreichenden Optionen auf Ein-, Tief- und Überblicke könnten nicht zutiefst private oder politische Bereiche der Beschäftigten erfassen (z. B. die persönliche Zufriedenheit, die politische Einstellung oder die Wahrscheinlichkeit von Streiks).

8 https://learn.microsoft.com/de-de/viva/glint/setup/gdpr-special-categories

Insgesamt muss sich jedes Unternehmen fragen, zu welchem Zweck Viva eingesetzt werden soll, ob die Viva-Apps den Zweck tatsächlich erfüllt und ob dieser Zweck nicht mit anderen, bereits vorhandenen Mitteln ausreichend erfüllt werden kann.

In einem Betrieb wurde zu Viva eine Betriebsvereinbarung abgeschlossen, die ausführlich darstellt, welche Kontrollmöglichkeiten die App beinhaltet. Außerdem stellte der BR in Versammlungen die BV vor und empfahl den Kolleg:innen, sie zu deaktivieren.

Die Verwendung von Viva Insights durch Mitarbeiter:innen steht jederzeit auf einer freiwilligen Basis. Die Teilnahme kann nicht durch lokale oder konzernale Führungskräfte vorgeschrieben werden. (...) Die Weitergabe von personenbezogenen Daten ist nicht erlaubt. ENDE

**Falls Viva bzw. einzelne Module davon verwendet werden sollen, wäre in der BV zu bestimmen:**

- Enge Zweckbindung; wozu wird Viva eingesetzt (z. B. Angebote für Lerninhalte sehen, öffentlich relevante Informationen bereitstellen und sehen)
- Freiwilligkeit klären (insbesondere bei „persönlichen Einblicken“ in Viva Insights)
- zu kommunizierende Inhalte festlegen (z. B. keine Krankmeldungen, Schichtpläne etc.)
- grundsätzlicher Verzicht seitens Vorgesetzter personen- und kleingruppenbezogener Analysen zu nutzen (z. B. bei Wahrnehmung von Schulungsangeboten, Beteiligung am Schwarzen Brett, Besprechungsgewohnheiten etc.); ausschließlich anonyme Personengruppen anzeigen
- arbeitsrechtliche Maßnahmen, die auf Auswertungen von Viva basieren, für unwirksam erklären

Die Gruppengrößen für Auswertungen bei Viva Analytics sollten von den Systemadministrator:innen möglichst groß festgelegt werden.

Betriebsratsmitglieder sollten sich regelmäßig vergewissern, dass diese Gruppengrößen beibehalten werden und keine Rückschlüsse auf einzelne Beschäftigte zulassen.

Der Betriebsrat kontrolliert regelmäßig, ob das Rollenkonzept von Viva passt, ob also Zugriffe auf die verschiedenen Apps von Viva tatsächlich nur von jenen Personen erfolgen, die dafür freigeschalten sind.

- Schulungen; insbesondere zu datenschutzrechtlichen Themen (z. B. Klassifikation und Vertraulichkeit von Informationen, Meinungsfreiheit, Profilingverbot etc.)

## TODO

Mit ToDo kann sich jede/r Nutzer:in Listen mit Tages- und Wochenplan erstellen (lassen). Die ToDo-Liste beinhaltet was zu tun ist, zusammengefasst aus anderen Apps (z. B. Kalender und Emails von Outlook [S. 41], Planner [S. 56], Teams [S. 43]). Vor der Aktivierung von ToDo sollte man abklären, ob andere Apps für die Arbeitsorganisation bereits in Verwendung bzw. besser geeignet sind.
Gesehen wird von Admins nur; ob die App verwendet wird, nicht was damit angezeigt wird.

Seit Herbst 2024 wird ToDo mit der „intelligenteren“ App „**My Day**“ [S. 56] ergänzt.

**In einer BV empfohlen:**

- Freiwillige Nutzung
- Ausschließlich persönliche Einsicht festlegen, insbesondere für den „intelligenten persönlichen Tagesplan“

## STREAM

Auf dem Videoportal Stream können firmenintern Videos hochgeladen werden. Stream ist für interne Kommunikation, Information und Schulung gedacht.

Stream liefert (derzeit) keine personenbezogenen Daten. Es wird zwar bekannt gegeben, dass etwas hochgeladen wurde, aber nicht von wem. Es wird angegeben, wie oft Videos angesehen wurden, aber nicht von wem. Es kann beobachtet werden, welche Teile eines Videos besonders häufig angesehen werden oder ob Zuseher:innen bei bestimmten Teilen besonders häufig wegklicken.

Für sich genommen wäre Streams einfach eine formatspezifische Plattform für Film-Dateien. Die Verknüpfung mit anderen Apps macht Stream zu einem vielseitigen Instrument. Über die App **Clipchamp** können Videos bearbeitet werden. Wer möchte, kann damit Bilder zuschneiden, Personen ausschneiden, Sequenzen überblenden, Audio hinzufügen etc. Mittels **Copilot** [S. 62] können Untertitel geschaffen, Transkripte ergänzt, Kapitel eingefügt, Übersetzungen und viele weitere Features eingebaut werden.

**In der BV festgelegt werden sollte:**

- Verantwortlichkeit (wer darf welche Videos für welche Beschäftigtengruppen hochladen)
- Zweckbestimmung (z. B. Schulungen und Marketing-Videos: ja, Videos von der Weihnachtsfeier nach 24h: nein)
- Videos bearbeiten, hochladen, ansehen, aktualisieren zählt zur Arbeitszeit
- Nutzung von Bearbeitungstools klären
- Zustimmung der auf den Videos abgebildeten Personen einholen
- Speicherdauer
- Ausschließlich unternehmensinterne Nutzung und Ansicht der Videos
- Allfällige Zugangsbeschränkungen (wer kann sich welche Videos ansehen)

## PLANNER

Planner ist eine App zur Projektarbeit. Im Planner können Projekte angelegt, Aufgaben verteilt und einzelne Schritte dargestellt werden. Alle Team-Mitglieder sind berechtigt, im Planner Projekte einzutragen, abzuändern und abzuschließen. Jede und jeder kann bestimmte Aufgaben nach selbst definierten Kategorien erstellen und bestimmte Personen den einzelnen Arbeitsschritten zuordnen, sie sozusagen mit der Erledigung bestimmter Projektschritte beauftragen. Typische Elemente in Planner sind Startdatum, Deadline, Status, Unteraufgaben, zugeordnete Personen und Anhänge.

Wird etwas verändert (z. B. eine Aufgabe umbenannt, eine Person anders zugeordnet) poppen diese Änderungen – je nach Einstellung – in den Outlook- Kalendern, ToDo-Listen oder Postfächern der Team- Mitglieder auf, weil die Apps miteinander verknüpft sind. Planner bietet in einem Diagramm den Überblick, was von den einzelnen Projektteam-Mitgliedern erledigt ist, was noch erledigt gehört, wer wann seine/ihre Aufgeben erledigt hat – und wer säumig ist.

Nachdem Planner ähnliche Funktionen hat, wie die MS Plattform **Project**, müsste im Betrieb nicht beides parallel im Einsatz sein. Auch **ToDo** hat eine ähnliche Zielsetzung – ist allerdings eher für Einzelpersonen gedacht. Eine eindeutige Abgrenzung zwischen den Apps ist daher hilfreich.

Seit November 2024 wird eine zusätzliche Funktion namens „**My Day**“ angeboten. Diese stellt ebenfalls projektbezogene Informationen dar. Dieser persönliche Tagesplan kann über Outlook geteilt werden und greift auf die hinterlegten Arbeitsstunden und angegebenen Arbeitsorte zu. Wer ist im Homeoffice? Wer ist außerhalb des Betriebes unterwegs? Wer ist Teilzeit beschäftigt? Diese Daten in My Day sollen der besseren Koordinierung zwischen den Beschäftigten dienen. Der Unterschied zu ToDo liegt darin, dass „My Day" als Liste für einen Tag angelegt ist, während die allgemeine To-Do-Liste als umfassender Aufgabenspeicher fungiert. Mit „My Day“ soll man sich - mittels Prioritätensetzung einer KI – auf die wichtigsten Aufgaben des Tages fokussieren.

**In der BV zu Planner sollte geregelt werden:**

- Die Zwecke festlegen in Abgrenzung zu anderen

Apps, die ebenfalls zur Prozessgestaltung verwendet werden können (z. B. Kalender, ToDo, Project, Teams)

- Berechtigungen beschränken (z. B. Projektgruppe)
- Festlegen, wer Aufgaben und Termine an andere (verpflichtend) verteilt
- Keine Vergleiche zwischen Projektgruppen oder gar Personen zulassen
- Festlegen, ob auch private Termine einfließen (z. B. Betreuungspflichten)
- Festlegen welche Angaben zu den einzelnen Aufgaben gegeben werden dürfen (z. B. in Arbeit/ erledigt/ verabsäumt/...)
- Festlegen, ob die Arbeitsleistung mittels Planner ausgewertet werden soll (z. B. wer versäumt besonders oft Deadlines oder wer setzt besonders oft Deadlines fest, die besonders oft versäumt werden?)
- Keine arbeitsrechtlichen Konsequenzen aus Planner-Inhalten (z. B. versäumte Deadline, nicht-erledigte Aufgabe) ableiten

## BOOKINGS

Bookings ist eine Anwendung, die primär zur Terminplanung in Unternehmen konzipiert wurde. Die Kernfunktion besteht darin, die Kalender der Mitarbeiter:innen so zu verwalten, dass Kund:innen, Klient:innen oder Geschäftspartner:innen eigenständig persönliche Termine buchen können.
Es können Termindetails hinzugefügt werden (z. B. Word-Datei mit einem Protokoll, Fotos etc.), die dann gemeinsam mit der Buchung gespeichert werden. Mit Bookings werden also virtuelle Termine via Teams [S. 43] organisiert und die Anwendung kann an verschiedene Branchen (z. B. Finanzdienstleistungen, Gesundheitswesen und Einzelhandel) und typische Situationen im Unternehmen angepasst werden.

### Tipps zur Regelung

- Speicherdauer festlegen (z. B. halbes Jahr nach Ablauf des gebuchten Termins); nicht vergessen: die (etwa auf Exchange gespeicherten) Zusatzinformationen benötigen ebenso eine Speicherfrist
- Reports festlegen (z. B. keine namentlichen Vergleiche, wer besonders häufig gebucht wird)
- Nutzung der „persönlichen Buchungen" freiwillig gewähren
- Zugriff auf den Buchungskalender einschränken

Administrator:innen können Bookings deaktivieren bzw. Gruppenrichtlinien einrichten und somit festlegen, wer neue Bookings-Kalender erstellen kann, wer Zugriff auf den Bookings-Kalender hat und wer die Rolle „Administrator:in" oder „Viewer:in" erhält. Für den Betriebsrat wäre zumindest eine lesende Rolle empfehlenswert.
Administrator:innen mit der entsprechenden Berechtigung können eine Liste aller Bookings-Postfächer in Exchange und Entra ID anzeigen. Damit ist eine Übersicht gewährleistet und der Betriebsrat kann diese nutzen, um die Einhaltung der Betriebsvereinbarung zu überprüfen.

## DYNAMICS

Dynamics ist ein zusätzliches Programm, das von MS vertrieben wird und hier der Vollständigkeit halber erwähnt ist, um zu zeigen, wie umfassend die Produktpalette von MS ist und dass bislang in Europa unübliche Anwendungszwecke (nämlich das Personalwesen) nach und nach ins Angebot integriert werden.

MS Dynamics ist eine Software für EPR (Enterprise Ressource Planing), HR (Human Relations) und CRM (Customer Relations Management). Dynamics bietet Funktionen für die traditionelle Personalverwaltung (z. B. Lohnverrechnung, elektronischer Personalakt, Arbeitszeiterfassung, Dienstreisenabrechnung, Urlaubsantrag, Rekrutierung und Kündigung, Qualifikation und Weiterbildung, Finanzberichterstattung, etc.).

Dynamics beinhaltet ein **Self-Service** für Beschäftigte und eigene Module für den Außendienst (sogenannte „**Field Services**") oder das Kundenmanagement

(sogenannte „CRM"). Bislang ist Dynamics in Österreich noch nicht allzu weit verbreitet, was vermutlich daran liegt, dass sich rechtliche Vorgaben und Unternehmenskultur im Mutterland von MS, den USA, deutlich von denen in Europa unterscheiden.

MS „**Customer Service**" ist ein Teil von MS Dynamics und bietet an, dass aus Social Media stammende Daten (z. B. Posts auf Facebook, Bewertungen auf Instagramm etc.) verarbeitet und so die Beziehungen von Beschäftigten und Kund:innen untereinander „besser" analysiert werden. „Customer-Experience (CX)" und „Service Solutions" sind Schlagwörter, die in diesem Zusammenhang fallen. Solche Informationen erfassen die Privatsphäre, spätestens wenn die Beschäftigten selbst Kund:innen des Unternehmens sind, und ihre Verwendung ist daher besser zu unterbinden.

**In einer BV ist zu regeln:**

- Klare Begrenzung wofür Dynamics verwendet wird (z. B. Reisekostenerfassung)
- Zugriff für Auswertungen, Auszahlungen und Aktualisierungen ausschließlich für Personal- oder Finanzverantwortliche
- Zugriff für die Beschäftigten auf ihren eigenen Account (Employee-Self-Service-Portal) ohne fremde Zugriffsmöglichkeit
- Einsicht für den BR zur Kontrolle
- Auswertungen grundsätzlich ohne Personenbezug (z. B. Lohnsummen, Verkaufssummen, Überstundensummen, Verkaufsprognosen etc.)
- für personenbezogene Auswertungen (neben den gesetzlich vorgeschriebenen) Anlassfälle definieren
- Keine Verwendung besonderer Datenkategorien (darunter versteht man Gewerkschaftszugehörigkeit, Gesundheit, sexuelle oder religiöse Orientierung, politische Meinung)
- Keine automatisierte Entscheidungsfindung! (z. B. wer wird befördert/gekündigt)

## FORMS

Forms ist eine einfach zu handhabende Software für das Erstellen von Umfragen. Die App kann für alle möglichen Interessen eingesetzt werden, um beispielsweise etwas über das Betriebsklima zu erfahren, um einen Termin zu koordinieren oder auch um Wünsche an die Betriebsratsarbeit zu erfragen. Beim Versenden der Umfrage können Links oder QR- Codes als Zugang mit verschickt werden.

Als einfache Faustregel für gute unternehmensinterne Befragungen gilt:

1., Die Fragen müssen einen Bezug zum Arbeitsleben haben.

2., Die Fragen sollen gut verständlich und neutral formuliert sein.

3., Die Auswertung sollte statistische Mindeststandards an Verlässlichkeit (also ohne Mess- oder Zufallsfehler) und Repräsentativität (also die Merkmale aller Beschäftigen widerspiegeln) erfüllen.

Daher ist 4., eine Schulung jener Arbeitnehmer:innen, die Umfragen erstellen und auswerten, sinnvoll.

Berücksichtigt man bei Befragungen zumindest diese Punkte, zeigt man, dass sensibel mit den wertvollen Daten der Beschäftigten umgegangen wird. Haben sämtliche Beschäftigten Zugang zu Forms, erzählen Betriebsrät:innen, dass es „inflationär" genutzt wird. Kolleg:innen wollen „ausprobieren", damit „spielen", erstellen und verschicken Umfragen relativ beliebig. Das Erstellen, Beantworten, Korrigieren, Auswerten und Befragungen sollten ernstgenommen werden. Das gelingt, wenn sie nicht inflationär ausgesendet werden und wenn sie von ausgewählten und geschulten Kolleg:innen interpretiert werden.

Auf Forms ist es möglich, eine **zeitliche Frist** festzulegen, um nachzuhaken, wenn etwa die Rücklaufquoten nicht den Erwartungen entsprechen. Eine zeitliche Abfolge festzulegen, wann eine Befragung beginnt, wann sie endet, wann die Ergebnisse im Betrieb veröffentlich werden, und wann Einzelergebnisse wieder gelöscht werden, ist ratsam.

Das mit den Antworten mitgelieferte Excel zeigt Uhrzeit

und E-Mail-Adresse zu jeder einzelnen Rückmeldung. Damit ist nachvollziehbar, wie lange für das Ausfüllen gebraucht wurde, wann ausgefüllt wurde, wer rückgemeldet hat etc. Diese Liste darf nicht zu Interpretationen über Arbeitsleistung oder Engagement herangezogen werden. Die Ergebnisse einer Umfrage gehören in der Regel nicht individuell dargestellt, sondern nur in absoluten Zahlen oder Prozentangaben, also statistisch. (Statistische Tests mittels Excel könnten sinnvoll sein, um einer Umfrage mehr wissenschaftliches Gewicht zu verleihen (z. B. Vergleich zweier Gruppen mittels sogenanntem „T-Test")).
Eine namentliche Umfrage auf Forms bietet keinen Schutz der Privatsphäre.

Folgende Einstellungen ermöglichen anonyme Umfragen

- „Namen erfassen" deaktivieren
- „Einzel-Ergebnisse anzeigen" deaktivieren

**Abstimmungen und Beschlüsse des Betriebsratsgremiums sollten nicht auf Forms stattfinden**, da es unter Umständen nicht gänzlich vor Zugriffen von Nicht-Befugten geschützt ist und das Ergebnis somit nicht rechtskonform wäre. Voraussetzung für das Fassen gültiger Beschlüsse auf Forms innerhalb eines Betriebsratsgremium wäre, dass die Identität der Mitglieder zweifelsfrei festgestellt wird, keine Beeinflussung stattfindet, die Ergebnisse revisionssicher aufbewahrt werden und fremde Einsichtnahme garantiert unterbleibt.

**Für die Verwendung von Forms sollte in einer BV geklärt sein:**

- Zweck der Umfrage
- Berechtigungskonzept; Wer darf Umfragen erstellen? Wer darf Umfragen auswerten? Wer kommuniziert die Ergebnisse den Beschäftigten?
- Verantwortlich Personen schulen
- Einbindung des BR
- Zeitliche Fristen (z. B. Speicherfristen, Genehmigungsprozess, Rücklauffrist...) sowie Aufbewahrungsdauer festlegen (engl.: „retention policy")
- Die Excel-Ergebnis-Sheets in einem verschlüsselten Bereich ablegen
- Ergebnisse im Betrieb statistisch kommunizieren

In einem internationalen Betrieb, in dem halbjährliche Umfragen an alle Beschäftigten weltweit ausgesendet werden, wurde dazu eine BV verfasst:

Vor Durchführung einer Umfrage werden die Beauftragten der Betriebsräte der von der Umfrage umfassten Betriebe über die anstehende Umfrage informiert und ihnen die Möglichkeit über ihre turnusmäßigen BR-Sitzungen eine Stellungnahme abzugeben bzw. die Umfrage zu genehmigen.

Die Teilnahme an der Umfrage erfolgt freiwillig. Die eingehenden Antworten werden ausschließlich in anonymisierter Form gesammelt und dem Auftraggeber konsolidiert zur Verfügung gestellt.

Die Nutzung oder weitere Verarbeitung der Umfrageinhalte ist ausschließlich für den vorab definierten Zweck gestattet. Eine nachträgliche

Zweckänderung ist nur nach vorheriger Rücksprache mit dem Betriebsrat gestattet.

Die Löschung von personenbezogenen Daten von Beschäftigten in Umfragen erfolgt unverzüglich, sobald der Zweck erfüllt ist, spätestens aber nach 30 Tagen. Verantwortlich hierfür ist der Ersteller der jeweiligen Umfrage. Lediglich die Ergebnisse ohne Personenbezug können auch weiterhin gespeichert werden.

## ONEDRIVE

OneDrive ist ein individueller Bereich zum Ablegen von Dateien aller Art. (z. B. Text, Musik, Fotos etc.). Ordner auf OneDrive können selbst definiert und die Inhalte mit selbst ausgewählten Personen geteilt werden. Die Dateien können zusätzlich verschlüsselt werden.

Da es sich um eine Anwendung in der Cloud handelt, können Nutzer:innen von unterschiedlichen Orten jederzeit auf die Inhalte zugreifen.

Hat man weiteren Personen den Zugriff erlaubt, können Dateien gemeinsam angesehen und bearbeitet oder geteilt werden.

OneDrive Wird als persönlicher Speicherbereich für Benutzer:innen zur Verfügung gestellt. Wenn ein Benutzer gelöscht wird, wird das OneDrive Laufwerk noch für 90 Tage gehalten und dann automatisch gelöscht. Die Nutzung von OneDrive wird erst nach entsprechender Mitarbeiterschulung freigegeben, Zusätzlich werden Compliance Regeln angelegt [Anm: und deren Einhaltung von der IT-Abteilung überprüft], um die Sicherheit von Daten zu gewährleisten.

Administrator:innen haben nicht automatisch Zugriff auf die OneDrive-Accounts von Beschäftigten. Was prinzipiell von Vorteil ist, weil keine unberechtigte Einsicht oder Abänderung durch Administrator:innen passieren kann, erweist sich in Notfällen, wenn Dateien von anderen Personen als den OneDrive-Besitzer:innen dringend benötigt werden, als Nachteil. Dieses Zugriffsverbot für Administrator:innen kann im „Compliance Manager“ [S. 66] umgangen werden.

Nutzer:innen, die die Berechtigung „**Websitesammlungsadministratoren**“ haben, können nachprüfen, ob und wer sich bei ihrem OneDrive Zutritt verschafft hat. Dazu kommt man über die im Menüpunkt „Berechtigungen“ in der Anwendungsverwaltung Entra ID [S. 78].
Auf **SharePoint** [S. 67]. hat ein Websitesammlungsadministrator immer Vollzugriff auf den Inhalt der ihm oder ihr zugeordneten Websitesites, kann also eine Einsichtnahme prüfen.
Außerdem tauchen sämtliche Zutritte auch im Protokoll der **Purview** Security & Compliance auf [S. 74]. Auf diesem Wege könnte man allfällige Einsichtnahmen überprüfen.

**In einer BV empfehlenswerte Regelungen:**

- Regeln für welche Dokumente OneDrive – nicht – verwendet wird (z. B. keine Personalakten) abgrenzen zu Sharepoint und Teams

- Privatnutzung regeln (z. B. solange der Arbeitsablauf nicht gestört ist und kein mutwilliger Schaden herbeigeführt wird, ist die Nutzung von OneDrive für private Zwecke zulässig). Sollte die Privatnutzung untersagt sein, ist zu regeln, wie dies kontrolliert wird.

- Zugriff regeln (Wer darf Einsicht nehmen? Wer darf im Abwesenheitsfall als Vertrauensperson Dokumente aus OneDrive sehen? Gibt es Gruppen auf OneDrive? Ist alles für alle offen? Wird regelmäßig überprüft, wer sich wessen OneDrive angesehen hat? Dürfen Dateien auch außerhalb des Betriebs geteilt werden?

- Aufbewahrungsdauer festlegen („retention policy“), spätestens mit Austritt aus dem Unternehmen sollte der Account in absehbarer Zeit gelöscht werden

- Freiwilligkeit vereinbaren, falls OneDrive nicht beruflich genutzt werden muss


MS 365 verlangt nicht, dass Texte, Bilder, Sprachaufnahmen etc. auf OneDrive abgelegt werden. Es können externe Angebote genutzt werden (z. B. Nextcloud, siehe Alternativen zu MS 365 im Anhang [S. 83]).

## VISIO

Visio wurde von MS 2000 gekauft. Es ist also bereits lange Teil der MS-Welt aber nicht im Standardpaket von MS 365, muss also eigens gekauft werden.

Mit Visio werden Grafiken erstellt, technische Zeichnungen angefertigt, Diagramme angeordnet, Prozesse visuell abgebildet und exportiert. Die Darstellungen von Visio basieren auf Datenbankabfragen im Hintergrund, die beispielsweise auf die IT-Infrastruktur zugreifen, um ein Flussdiagramm zu erstellen.

Mehrere Personen können an einem Bild arbeiten.

**Zu regeln ist**

- Zugriff; Wer darf welche Diagramme sehen/bearbeiten/weiterleiten? Was darf wohin exportiert werden?

## DELVE

„Delve ist seit 2015 ein fixer Bestandteil von MS 365." Lautete der erste Satz zur App Delve in der Ausgabe dieser Broschüre von 2023. Die App wurde mit Dezember 2024 eingestellt. Sie enthielt die Möglichkeit, Dateien nach „Wichtigkeit" zu filtern. Diese Möglichkeit besteht nun im Windows Explorer (durch drücken auf die Windows-Taste und den Buchstaben E auf der Tastatur) in den Optionen „Empfohlen" oder den selbst bestimmten „Favoriten". Dies ist auch in einigen anderen Anwendungen möglich (siehe Viva [S. 52], Teams [S. 43]). Ausschalten von Delve ist somit keine Garantie dafür, dass dessen Funktionen auch ausgeschalten sind – diese sind lediglich in andere Anwendungen übergegangen. Delve ist ein gutes Beispiel dafür, wie die Welt von Microsoft permanent verändert wird.

## SKYPE

Skype hat ein bewegtes Leben hinter sich und brachte es darin sogar zu einem eigenen Vokabel – „skypen" steht im Duden für Echtzeit-Telefonie im Internet mit Video. 2003 als Unternehmen gegründet, wurde Skype Technologies 2011 von Microsoft gekauft. Von 2010 bis 2015 gab es die Echtzeitkommunikation von MS unter dem Namen „LYNC". Bis 2013 gab es zum „tratschen mit Video" den „Live Messenger". Für Skype ist 2021 das Ende gekommen. Echtzeitkommunikation in Ton und Bild findet auf Teams statt [S. 43]. Wird bald „geteamst" statt „geskypt"?

## SPRACHASSISTENZ

Was „Alexa" für Amazon und „Siri" für Apple, das war „Cortana" für Microsoft – Sprachassistenz. Cortana selbst gibt es nicht mehr, doch ist Spracherkennung in einigen Anwendungen integriert. Es muss nicht „Cortana" draufstehen, damit Spracherkennung drin ist.
Mit der Sprachfunktion können MS 365-Apps gesteuert, oder Text diktiert werden. Mit dabei ist KI. Die Sprachfunktion kann Termine in Outlook [S. 41] eintragen, an die To-Do-Liste [S. 55] erinnern, bei der MS-eigenen Suchmaschine Bing [S. 62] nachfragen, Dokumente auf Onedrive [S. 60] suchen etc.

**Beim Einsatz von Sprachassistenz wäre zu klären:**

- Zwecke
- Freiwilligkeit
- Information und Unterweisung der Beschäftigten (z. B. dass Sprachassistent aktiviert ist, Daten gespeichert werden, Daten analysiert werden, das Programm mit anderen Anwendungen verknüpft ist).

## SWAY

Bei Sway handelt es sich um eine App für Präsentationen. Videos, Text in verschiedensten Formatierungen sowie Karten, Tabellen oder Musik können hier zu ansprechenden Darstellungen zusammengebaut werden. Ein Nutzer sieht in der einfachen Handhabung „gegenüber dem Funktionsmonster PowerPoint" einen Vorteil von Sway.

Sway kann für interne Schulungen, Werbung oder auch für Informations-Videos des Betriebsrats an die Belegschaft genutzt werden. Wer eine Präsentation erstellt hat, kann sehen, wie viele Nutzer:innen sie angesehen haben, wie viel Zeit sie dafür verwendet haben und ob die Darstellung bis zum Schluss angesehen wurde.

**In einer BV wäre zu klären:**

- Verwendungszweck klären (z. B. betriebsinternes Lernen)
- Berechtigungskonzept (wer darf hochladen, ansehen, löschen, verändern?)
- Rechte klären (gehören die Filme dem Unternehmen, denen, die sie hochladen, denen die darauf zu sehen sind, denen, die sie geschnitten haben?)
- Löschfristen (wie lange werden die Präsentationen/ Videos behalten?)

## BING

Die MS-eigene Suchmaschine erfreut sich wenig Aufmerksamkeit – außer sie wird von der französischen Datenschutzbehörde zu 60 Millionen Euro Strafe verurteilt, weil Einverständniserklärungen und Cookie-Banner zur Datenübertragung in die USA fehlen (Dezember 2022).
Bing sucht innerhalb der unternehmensinternen Anwendungen von MS 365 – wenn das so eingestellt wurde. Bing verwendet das, was firmenintern hochgeladen wird (z. B. auf Sharepoint [S. 67]). Hat man andere Anwendungen in Betrieb, mit denen verloren geglaubte Informationen wiedergefunden werden (z. B. Data Loss Prevention [S. 80]), ist Bing für diese Zwecke eigentlich nicht zusätzlich erforderlich.

## COPILOT

Die in einer Basisversion gratis im Netz verfügbare Künstliche Intelligenz (KI) **Chat GPT** wurde in einem US-amerikanischen Unternehmen namens „OpenAI" entwickelt dessen Leitung von der Gründung 2015 bis zu seinem Ausstieg 2018 der (derzeit) reichste Mann der Welt innehatte (Elon Musk) und an dem MS (derzeit) 49 % Anteile in der Stiftungskonstruktion hält und das

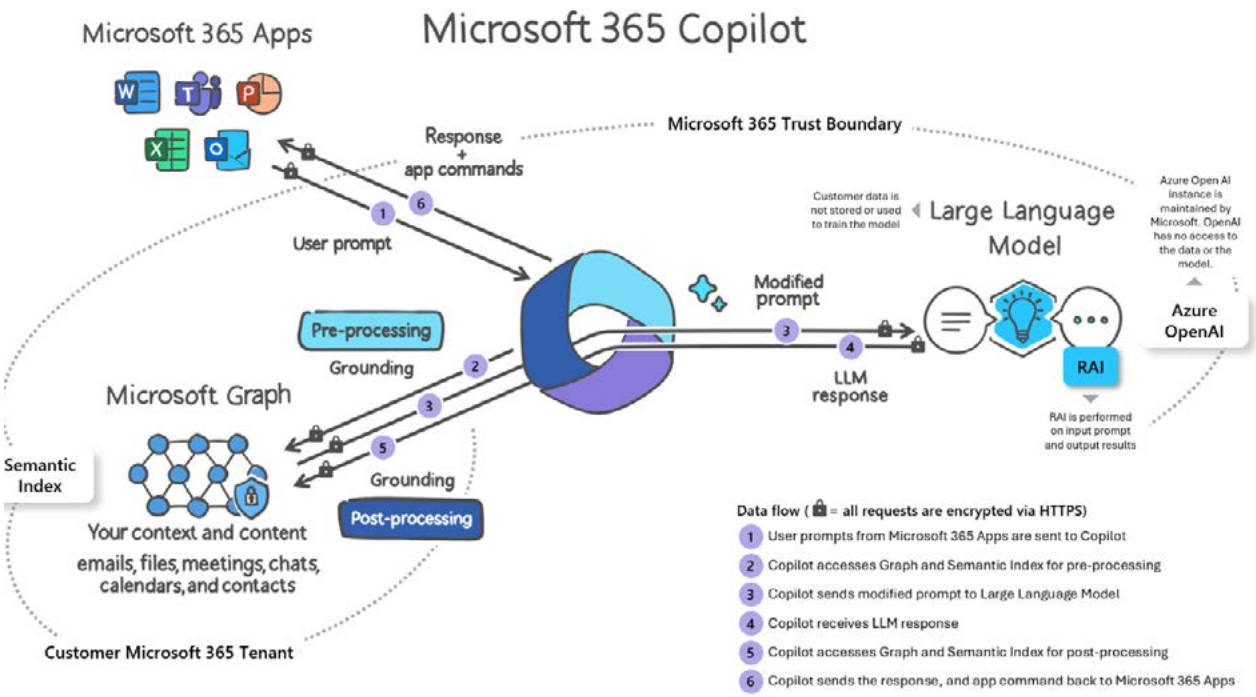
(derzeit) als das teuerste Startup mit einem Marktwert von 29 Milliarden Dollar gehandelt wird. Die Entwicklung der KI namens ChatGPT, auf der Copilot aufbaut, war MS den großzügigen Betrag von einer Milliarde Euro wert. Mit Stand Dezember 2024 muss Copilot um 22 Euro pro Lizenz zum Standard-Paket von MS 365 zugekauft werden. Es ist jedoch zu erwarten, dass Copilot standardmäßig in die Welt von MS 365 integriert wird.

Die Abkürzung ChatGPT steht für Chat Generative Pre-Trained Transformer, deutsch könnte man es bezeichnen als: „Unterhaltung erzeugender vorab ausgebildeter Umwandler". Copilot für Microsoft 365 basiert auf ChatGPT, einem sogenannten **Large Language Models (LLM)**. LLM ist ein KI-Modell, das mit umfangreichen Daten trainiert wurde, um menschliche Sprache zu verstehen, zu generieren und kontextbezogene Antworten zu liefern. 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.
Die KI erfasst im Netz verfügbare Informationen und stellt sie ethisch trainiert zu neuen, für viele überraschend hochwertigen Texten, Gedichten, Geschichten oder Bildern zusammen. Egal ob Hausübung, Zeitungsartikel, eine Website samt Inhalt, ein Bild im Van-Gogh-Stil, ein Drehbuch, ein Reiseführer, ein Programmcode, eine Fehlersuche in der Programmierung etc., der Chatbot ist universal einsetzbar und erfreut sich großer Beliebtheit.

Mittels ChatGPT bzw. dessen „Nachfahre" Copilot werden derzeit in der Welt von MS die Suchmaschine Bing leistungsfähiger, Teams-Konferenzen besser zusammengefasst, von gesprochener Sprache in (fremdsprachigen) Text übersetzt etc. Als Unterstützung für sämtliche Microsoft 365 Dienste und mit den Funktionen der ehemaligen Sprachassistenz „Cortana" bestückt [S. 62], werden mit Hilfe von Copilot unternehmensintern Word-Dokumente in einem bestimmten Stil erstellt oder zusammengefasst, wiederkehrende Aufgaben in Excel-Tabellen automatisiert, E-Mails in Outlook nach ihrer Dringlichkeit organisiert [S. 41], Teams-Sitzungen transkribiert, protokolliert und übersetzt [S. 43] oder auch eine Aufgabenliste aus dem Kalender abgeleitet – um nur einige Beispiele zu nennen. Da alles, was mittels einer Anwendung von Microsoft 365 im Betrieb funktioniert, in die Berechnungen des Copilot einfließt, sind die Einsatzmöglichkeiten zahlreich.

Zusätzlich können Dienste von Microsoft wie die Suchmaschine Bing oder das Betriebssystem Windows 11 sowie sämtliche angedockte, also mit Schnittstellen (wie Graph-Konnektoren oder Teams Message Extensions)

**FUNKTIONSWEISE DES COPILOT**



eingebundene Systeme anderer Anbieter ebenfalls ausgelesen werden. So können Unternehmen je nach Wunsch und Bedarf Datenquellen hinzufügen und den Inhalt, auf den Copilot zugreift, beliebig erweitern.

Eine Interaktion mit Copilot beginnt mit einem sogenannten „user prompt", der Frage eines Nutzers bzw. einer Nutzerin, die einem Suchbefehl gleichkommt. Diese Anfrage wird einer ersten Verarbeitung (Grounding) unterzogen, wobei betriebsinterne Informationen aus MS Graph [S. 69] und allfällig vorhandenen externen Erweiterungen hinzugezogen werden. Microsoft Graph spielt eine zentrale Rolle, indem es Daten aus verschiedenen MS 365-Quellen wie E-Mails, Dateien und Kalendern bereitstellt.
Nach der Vorverarbeitung wird die verfeinerte Anfrage an das LLM gesendet, das von Azure OpenAI betrieben wird. Das Unternehmen Open AI hat laut Microsoft keinen Zugriff auf die Daten, da diese innerhalb der von MS betriebenen Infrastruktur Azure ausgewertet werden.
Die fertige Antwort von Copilot basiert auf der Anfrage und dem verfügbaren Kontext und 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 geknackt werden könnte. Manchmal enthalten diese „Hacks" eher banale bis amüsante Umgehungen von ethischen und moralischen Grundsätzen, wie die Aussicht auf virtuelles Trinkgeld. Sie können jedoch auch mit „emotionalem" Druck unethische Antworten herausfordern indem beispielsweise behauptet wird, man sei in Lebensgefahr, wenn man diese oder jene Information nicht bekommen würde.

Empfohlen sei Unternehmen eine konkrete Anwendung von Copilot erst nach einer ausgiebigen **Testphase**.

Copilot wird Stück für Stück auf den Markt gebracht und erweitert. Im Herbst 2024 wurde das **Copilot Studio** an den Mann und die Frau gebracht (eine frühere Anwendung, konnte ähnliches und hieß Power Virtual Agents). Damit kann ein Betrieb selbst „Agenten" erzeugen, die auf die betrieblichen Wünsche exakt abgestimmt sind. Für das Copilot Studio benötigt man keine oder wenn, nur sehr wenig Programmierkenntnisse (man nennt das „noCode – lowCode"). MS schreibt, dass Copilot insbesondere im HR-Prozess nützlich ist und nennt als Beispiel: „Mitarbeiterumfragen entwerfen, Umfragen analysieren, um wertvolle Einblicke in die Stimmung [!] der Mitarbeiter zu gewinnen."

Es gibt außerdem KI-gestützte **Copilot Agents**, die spezifische Aufgaben automatisieren. Die Einsatzbereiche der Copilot Agents umfassen unter anderem: Routinemäßige Berichte erstellen, Datenanalyse, proaktive Unterstützung bei Kund:innenanfragen (z. B. Weiterleiten an die zuständige Person). Einem Agent kann eingegeben werden, in welchem Stil zu antworten ist. Dem Agent kann eingegeben werden, welche Abläufe zu befolgen sind oder auf welche Dokumente – nicht – zurückgegriffen werden soll (beispielsweise indem die als „top secret" klassifizierten Unterlagen aus Analysen ausgeschlossen werden). Copilot Agents zielen – laut MS – darauf ab, die „Produktivität zu steigern", „Arbeitsprozesse zu optimieren" oder die „Benutzererfahrung bei MS 365-Anwendungen zu verbessern". Agents seien wie Teammitglieder, so MS in einem firmeneigenen YouTube-Video, jeder Agent passe sich so an die User:innen an „wie der Hund dem Herrchen". MS wirbt, dass der Agent „wertvolle Kennzahl zur Beurteilung des Mitarbeiterengagements [liefere]. Sie [die Kennzahl] misst, wie wahrscheinlich es ist, dass Ihre Mitarbeiter Ihr Unternehmen ihren Freunden oder ihrer Familie als großartigen Arbeitsplatz empfehlen [!]."[9]. Engagement wird in Empfehlungen im Bereich der Privatsphäre gedacht. Das zeigt, wie wenig MS den Schutz der Privatsphäre berücksichtigt und wie stark Personalisierung und Emotionalisierung im Vordergrund stehen.

MS hat für bestimmte Zwecke bestimmte Agents vorprogrammiert. Die Unterstützung im Verkaufsprozess erfolgt durch sogenannte **Sales Agents**, die herausfinden, was dem/der Kund:in wichtig ist, welche Produkte wem angeboten werden könnten und Ähnliches. Unterstützung kann man sich auch mit dem sogenannten

9 https://adoption.microsoft.com/en-us/copilot-scenario-library/human-resources/

**Business Chat** holen. Dieser **BizChat** ist eine KI-gestützte MS 365-Anwendung, die Unternehmensdaten aus verschiedenen Quellen wie E-Mails, Dokumenten und Chats verknüpft und Beschäftigten helfen soll, schnell Informationen zu finden, Zusammenfassungen zu erstellen und komplexe Aufgaben zu bewältigen. Das Programm fungiert quasi als persönliche:r digitale:r Assistent:in.

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 innewohnt 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, egal ob Excel-Tabellen, Übersetzungen, Zusammenfassungen oder Protokolle 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.

Einige wichtige Fragen zwischen Betriebsrat:rätin und Geschäftsführung sollten beantwortet sein, wenn der Copilot im Betrieb zum Einsatz kommen soll.

**Was in einer Betriebsvereinbarung zu regeln ist**

- Für welche Zwecke soll der Copilot verwendet werden (z. B. Koordinieren von Terminen mit Kund:innen für den Außendienst, Erstellen von Protokollen nach Teams-Sitzungen)

- Gibt es Aufgaben, für die der Copilot keinesfalls eingesetzt werden darf (z. B. Zusammenfassung von als „streng vertraulich" klassifizierten Dokumenten)?

- Ändert sich die Anforderung an Qualifikationen von Arbeitnehmer:innen?

- Ändern sich die Arbeitsaufgaben? Werden Arbeitsaufgaben durch den Copilot ersetzt? Erfordert die Korrektur der Ergebnisse und Vorschläge von Copilot spezielle Kompetenzen?

- 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 allfällig erforderliche Klassifizierung, die Zuordnung der Dateien?

- Ist die Verwendung des Copilot freiwillig? (Natürlich ist juristisch im Arbeitsverhältnis kaum Freiwilligkeit gegeben und technisch fließen die Daten der Beschäftigten in der Regel in den Copiloten mit ein, dennoch sollte geklärt werden, ob er verwendet werden muss. Und wenn „ja": von wem und wofür?)

- Müssen die Ergebnisse und Vorschläge umgesetzt bzw. befolgt werden (z. B. Prioritätensetzung bei Antworten auf Emails)? Wer ist verantwortlich für Ergebnisse, die Copilot zusammenstellt? Müssen Ergebnisse extra ausgewiesen werden (z. B. mit einem Vermerk „diese Präsentation wurde mit Hilfe von Copilot erstellt")?

- Gibt es Daten, Unterlagen, Aktivitäten von Personen die aus den Berechnungen ausgeschlossen werden sollten oder aufgrund rechtlicher Geheimhaltungspflichten ausgenommen werden müssen?

- Wie und an welcher Stelle ist der Betriebsrat eingebunden?

- Wurden die Nutzer:innen für die Anwendung geschult? Erfolgt die Schulung bzw. das Ansehen von Schulungsmaterial (z. B. YouTube-Videos) während der Arbeitszeit?

- Gibt es eine oder besser mehrere eigens qualifizierte Personen im Unternehmen, die für Fragen der Anwender:innen zur Verfügung steht (z. B. Copilot-Expert:in)?

# ANWENDUNGEN FÜR ADMINS

## EINE AUSWAHL AUS DEM BACKEND

Die hier beschriebenen Programme, Anwendungen und Plattformen stellen eine Auswahl der gebräuchlichsten Dienste von MS 365 dar, über die MS 365 als Ganzes funktioniert, die im Hintergrund laufen. Einzelne Nutzer:innen haben dazu in der Regel keinen Zugriff. Zu ihnen hat üblicherweise nur jemand mit Admin-Berechtigung Zugang. Es könnten auch Rechte an ausgewählte Nutzer:innen, wie etwa Betriebsrät:innen vergeben werden. Es kommt darauf an, wie das Berechtigungskonzept betriebsintern festgelegt wurde, ob Zugang zu einer dieser Anwendungen besteht – oder nicht. Die Unterteilung in dieser Publikation in die Zielgruppen Nutzer:innen und Administrator:innen soll dem Betriebsrat bei der Orientierung helfen und dient der Übersicht über die wichtigsten dieser Anwendungen, welche Funktionen sie beinhalten, und nicht zuletzt wie sie sinnvoll gehandhabt werden können.

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, wer welche Änderungen vornehmen kann, das muss im „Backend", also im digitalen Hintergrund, in der Systemverwaltung, eingestellt werden.

An Führungskräfte sollten keine Admin-Rechte vergeben werden (Ausnahme ist die IT-Abteilung), damit diese sich keine personenbezogenen Auswertungen ansehen.

In der Funktion „role based exit controll" kann theoretisch jede beliebige Zugriffs-, Lese- und/oder Ansichtsberechtigung erstellt werden.

Privilegierte Nutzer, also jene mit Zugriff auf 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).

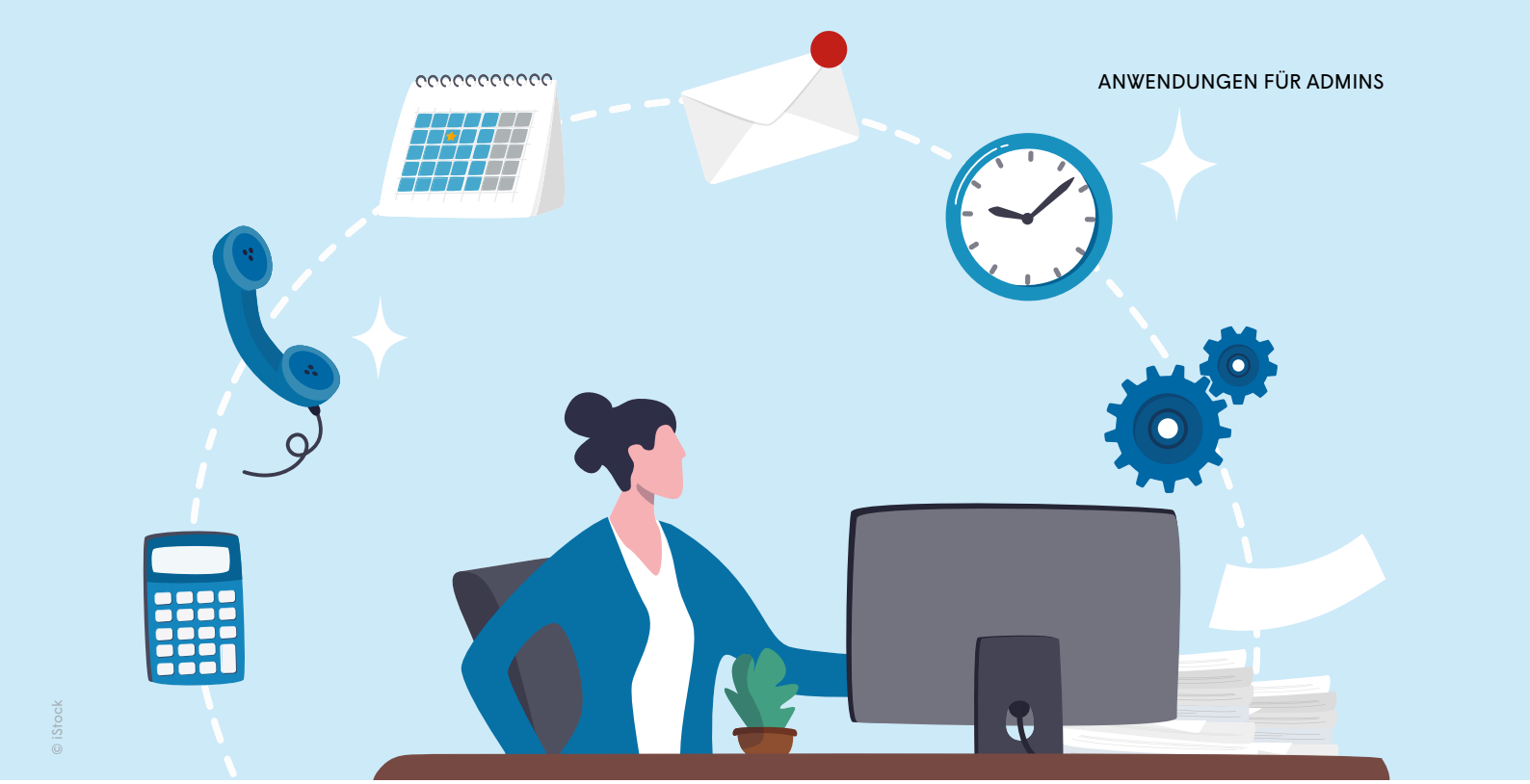
Die folgenden Kapitel enthalten graue Kästchen.

Jene mit einem Anführungszeichen beinhalten Beispiele aus bestehenden Betriebsvereinbarungen.

Jene mit Pfeilchen enthalten praktische Tipps.

Jene mit Diamanten Besonderheiten.

Am Ende jedes Kapitels sind die wichtigsten Punkte, die in einer Betriebsvereinbarung zur jeweiligen Anwendung behandelt werden sollten, aufgezählt.




## AZURE

Azure ist eine Cloudplattform. Auf Azure werden alle Online-Angebote von Microsoft abgewickelt. Es ist kein physischer Speicher vor Ort nötig. Azure ist *die* Online-Infrastruktur für Microsoft.
Im Jahr 2024 wurden KI-Anwendungen in Azure ergänzt. Im Dezember 2024 standen 273 verschiedene Services zur Verfügung (siehe https://azure.microsoft.com/de-de/products). Eine davon scheint besonders problematisch, da sie Stimmung und Verhalten auswertet und dazu auch mit personenbezogenen Daten außerhalb des Unternehmens arbeitet. Sie nennt sich **Azure Cognitive Services (ACS)** und MS schreibt dazu: „Um die Stimmung und Themen der Zielgruppe anzuzeigen, aggregiert Azure Cognitive Services (ACS) Beiträge und Kommentare aus Storylines und öffentlichen Beiträgen."

## SHAREPOINT

In diesem zentralen Bereich werden die gesamten MS 365-Anwendungen verwaltet. Über Sharepoint werden Benutzer:innen hinzugefügt und entfernt, Lizenzen und Berechtigungen geändert, Kennwörter zurückgesetzt. Über SharePoint können beliebige weitere Seiten eingerichtet werden (z. B. Dateisammlungen, Mailboxen, Workflows, Telefonverzeichnis, Kalender etc.). Im Grunde ist SharePoint ein riesiges Content-Management-System (CMS), auf dem unterschiedlichste Formate eingehängt werden können. Das Suchen nach Videos/ Personen/ Dateien funktionieren auch über SharePoint.

Eine Aufzählung, welche personenbezogenen Daten in SharePoint verwendet werden, schafft Transparenz und Vertrauen. Welche Daten in dieser mächtigen „Schaltzentrale" verwendet werden, wurde in einer Betriebsvereinbarung folgendermaßen geregelt:

> Neben den aus dem 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 Teamspaces
> 6. Freigabefunktion zur Beantragung einer Teamspace-Freigabe von Dokumenten
> 7. 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 auf SharePoint erstellt, genehmigt, genutzt werden dürfen.

Andernfalls sind Verwirrungen, Doppelgleisigkeiten, Wissensverluste und ähnlich unangenehme Vorkommnisse vorprogrammiert.

SharePoint sollte nicht von ungeübten Nutzer:innen eingerichtet werden können, sondern nur von ausgewählten, gut geschulten Entscheidungsträger:innen.

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

„Owner" einer Sharepoint Seite haben Zugang, zu personenbezogene Aktionen. „Als Websitebesitzer können Sie steuern, ob Personen die Namen von Personen sehen, die Dateien oder Seiten auf einer Website anzeigen," schreibt Microsoft.

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 wie in der unteren Darstellung.

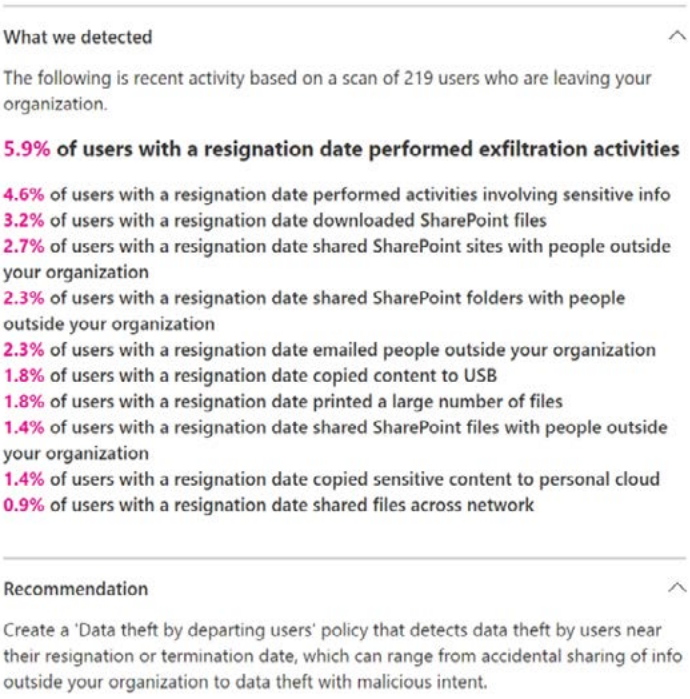
Das Anzeigen von namentlichen Benutzeraktivitäten ist im Überwachungsprotokoll des Purview-Compliance Portals [S. 74] ersichtlich und kann ausgewertet sowie dem Betriebsrat zur Verfügung gestellt werden.

Unter Einbindung des Betriebsrates kann im Bedarfsfall, also bei einem schwerwiegenden und begründeten Verdacht von 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.

Sharepoint als „Schaltzentrale" bringt es mit sich, dass Auswertungen von Sharepoint-Aktivitäten durchaus problematisch sein können.

In der Abbildung (unten) wird gezeigt, dass nach jenen Arbeitnehmer:innen gefiltert werden kann, die demnächst das Unternehmen verlassen. Diese werden untersucht, ob sie sensible Daten eingesehen, Daten von Sharepoint heruntergeladen, mit Personen außerhalb des Unternehmens geteilt, in großem Umfang ausgedruckt haben u.s.w. 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.

### WER DAS UNTERNEHMEN VERLÄSST, KÖNNTE DIEBSTAHL BEGEHEN



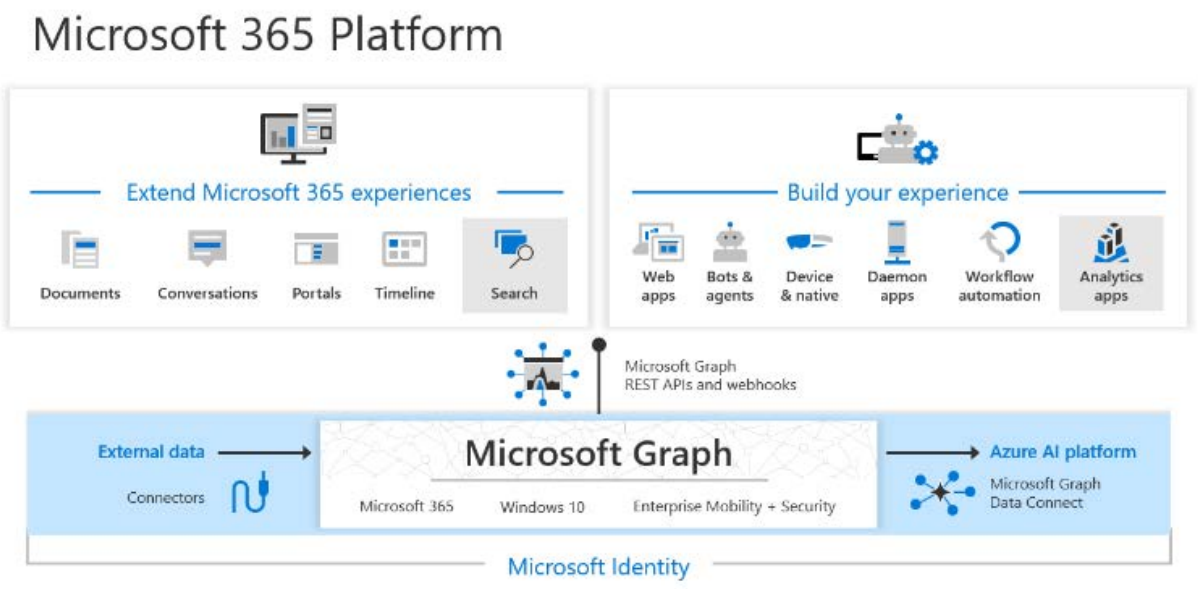
**In der BV sollte geklärt werden:**

- 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, filtern, ansehen?
- Eindeutige Zwecke
- Festlegen, welche Daten nicht auf SharePoint abgelegt werden sollen (z. B. mittels einer Datenklassifikation im „Security and Compliance Center")
- Festlegen wie viel Speicher für wen auf welchen Seiten zur Verfügung steht und die Nutzer:innen darüber informieren
- Schulungen für Anwender:innen
- Einsichtsrechte für den Betriebsrat
- Allfällig eingebundene externe Anwendungen und Schnittstellen darstellen und den jeweiligen Zweck bestimmen
- Nutzer:innenverhalten ohne Personenbezug analysieren und nur einem engen Personenkreis für einen konkreten Anlassfall zugänglich machen
- Folgemaßnahmen bei festgestelltem Fehlverhalten nur in Absprache mit dem Betriebsrat
- Löschkonzept

## GRAPH

Graph ist das „Herzstück" von MS 365. In Graph werden sämtliche Aktivitäten, Dateien, Metadaten, Inhaltsdaten u.s.w. aus allen anderen MS 365 Anwendungen zusammengeführt. Über Graph lässt sich feststellen, wer, wie lange, wie häufig, mit wem und mit welchen MS 365-Anwendungen mit welchen Einstellungen arbeitet. Graph speichert Telemetriedaten nicht selbst sondern greift auf andere Anwendungen zurück und stellt die Ergebnisse wiederum anderen MS-Diensten zur Verfügung. Graph stellt Beziehungen zwischen den riesigen Datenmengen der MS-365–Welt her.
Bei Graph können Schnittstellen eingebaut werden, wie beispielsweise eine Schnittstelle, die zur Sicherheit dient und Abweichungen von „normalen" Verhaltensweisen feststellt, auffälliges Verhalten unter „Quarantäne" stellt, also vom übrigen System isoliert, damit kein (weiterer) Schaden angerichtet werden kann und Alarm auslöst. (zur Funktionsweise von Security-Anwendungen siehe Purview [S. 74]).
Über Schnittstellen (Graph Connectors) können auch Apps außerhalb von MS 365 in Auswertungen integriert werden.

### FUNKTIONSWEISE VON GRAPH



Die permanente Datenerfassung durch Graph läuft immer. Zwar kann man verhindern, dass Auswertungen angezeigt werden – umfassende technische Verhaltens- bzw. Aktivitätskontrolle ist dem System von MS 365 durch die Konstruktion fix eingebaut.

Systemadministrator:innen könnten das so genannte „**Benutzeraktivitätsberichtsprotokoll**" auch dann einsehen wenn Nutzer:innen es nicht aktiv verwenden. In der BV sollte unbedingt ausgeschlossen werden, dass diese Überwachung seitens Vorgesetzter ohne Angabe von vernünftigen Gründen eingesehen wird oder gar negative Folgen für die Beschäftigten hat.

**Für die BV zu regeln:**

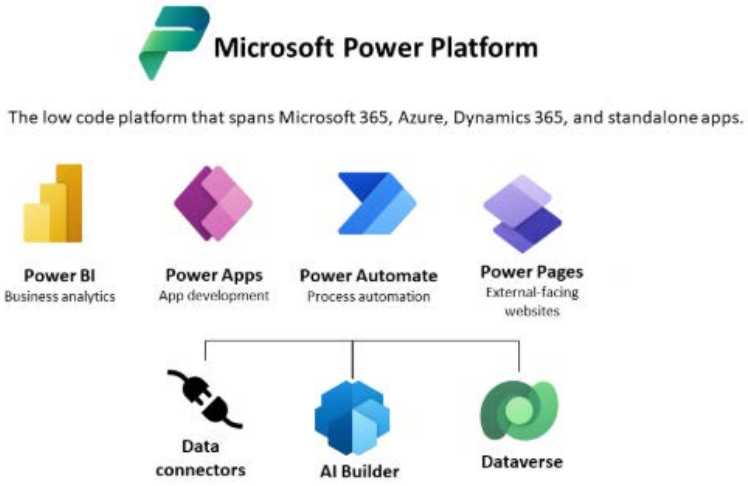
- Allfällig vorhandene Schnittstellen (so genannte Application Programming Interfaces, API) zu externen Programmen mit personenbezogenen Daten von Beschäftigten, sollten definiert werden und dürfen nur für eindeutig festgelegte Programme und Zwecke genutzt werden.

## POWER PLATFORM, POWER AUTOMATE & FABRICS

Mit den verschiedenen Power Apps kann man auf spezifische Zwecke zugeschnittene, innerbetriebliche Anwendungen kreieren; eigene Analysen, Workflows oder Datenbanken können über die Power-Apps zusammengestellt werden ohne genauere Kenntnis einer Programmiersprache. Letztes wird von MS als Vorteil herausgestrichen.

Power Platform besteht aus mehreren Komponenten (Power BI, Power Apps, Power Automate und Power Pages), die ihrerseits auf die gesamten Unternehmensdaten in MS 365 über das sogenannte **Dataverse** zugreifen können. Dataverse bezeichnet jenen Ort, wo alle Daten strukturiert aufbewahrt werden. Power Platform funktioniert über vorwiegend optische und somit einfach zu verwendende Bausteine zur Entwicklung von Programmen (sogenannte Low-Code-Entwicklungstools).

**DER STAMMBAUM DER FAMILIE „POWER"**




Ein „Familienmitglied" aus der Familie Power ist **Power BI**. Damit werden Daten aus den verschiedensten Quellen in- und außerhalb des Unternehmens analysiert und optisch dargestellt (z. B. Verkaufszahlen auf interaktiven Dashboards, Statistiken der historischen Lagerbestände kombiniert mit Wirtschaftsprognosen, Fluktuation der Beschäftigten etc.). Power BI kann unabhängig von Power Platform oder Fabrics erworben und genutzt werden (MS nennt das „stand alone service").

Die Mitsprache des Betriebsrats wurde in einer Betriebsvereinbarung so geregelt:

Bevor über Power BI automatisierte Berichte und Auswertungen erstellt werden, wird gemeinsam mit dem Betriebsrat festgelegt, ob Bedarf für derartige Anwendungen besteht und für welche Zwecke diese dienen sollen.

Es werden keine personenbezogenen Ergebnisse mit Power BI erstellt, sondern es umfassen diese immer Gruppen von zumindest zehn Personen. Es werden weiters keine personenbezogenen automatisierten Entscheidungen (ADM) getroffen.

Ergebnisse, Auswertungen und (grafisch aufbereitete) Ansichten von Power BI verbleiben inner

halb von Power BI, es erfolgt keine Übertragung in andere Formate oder Apps.

Die Erstellung von Berichten und Auswertungen in Power BI ist einem engen vorab geschulten und festgelegten Personenkreis gestattet.

In Power Automate können Berechtigte definierte Abläufe und Anwendungen ohne umfangreiche Programmierkenntnisse erstellen, wobei auf verschiedenste MS 365 Apps zugegriffen wird. Beispiele sind das Organisieren von E-Mail-Anhängen aus Outlook direkt in OneDrive oder eine Warnung, falls jemand unentschuldigt bei einer teuren Weiterbildung nicht erscheint oder das automatische Weiterleiten von Serviceanfragen an zuständige Teams und Eskalation an die zuständigen Manager:innen etc. Bei der Rechnungslegung können z. B. Informationen aus eingehenden Rechnungen nach bestimmten Kriterien herausgefiltert und automatisch in das Buchhaltungssystem zur Freigabe importiert werden. Die Problematik dabei ist, dass jene Personen, deren E-Mails, Nachrichten, Chats etc. in die Power App eingebaut werden, davon nicht zwangsläufig etwas erfahren.

Sind im Unternehmen auch KI-Anwendungen wie Copilot oder Azure AI in Betrieb, können deren Analysen in die neu geschaffene Anwendung mit einfließen.

**Wo „Power" drauf steht, kann „KI" drin sein**.

Microsoft **Fabrics** ist eine eigenständige Plattform und kein direkter Teil der Microsoft Power Platform. Allerdings gibt es eine enge Verbindung zwischen den beiden Systemen. Fabrics ist eine umfassende Anwendung für Datenanalyse und -management, die verschiedene cloudbasierte Dienste (auf Azure) in einer Umgebung zusammenführt. Fabrics greift auf Daten zu, die außerhalb der Unternehmens-IT im Internet verfügbar sind.

Dass sowohl Power Platform als auch Fabric auf das gesamte Dataverse, also alle in MS365 verfügbaren Datenbestände zugreifen, steigert deren Analysefähigkeiten. So können die Zugriffsberechtigten Daten aus Power Apps oder Dynamics 365 in Fabric erweitert um Daten aus dem WorldWideWeb analysieren und die gewonnen Erkenntnisse wiederum in Power Apps-Anwendungen einbinden. Fabric und Power Platform sind separate, aber eng miteinander verbundene Plattformen, die sich gegenseitig ergänzen und erweitern.

## AI BUILDER

AI Builder ist eine Zusammenschau mehrerer KI – Funktionen, die es ermöglicht, benutzerdefinierte Modelle für Spezialfälle zu erstellen und in Power Apps oder Power Automate zu integrieren. AI Builder arbeitet mit Hilfe von künstlicher Intelligenz, ohne dass man dafür programmieren können muss (diese, meist mit visuellen Bausteinen arbeitende Methode wird „low code/ no code" genannt). Mit Hilfe des AI Builders kann man zum Beispiel Informationen aus Dokumenten herauslesen, Bilder erkennen und sortieren oder auch Vorhersagen treffen (z. B. welche Kund:innen wahrscheinlich etwas kaufen werden). KI könnte für die Schadenserkennung eingesetzt werden, indem anhand von Bildmaterial trainiert wird, Schäden an Produkten oder Geräten zu erkennen.

Es ist entscheidend, im Vorhinein festzulegen, zu welchem Zweck Anwendungen in der Power Platform erstellt werden sollen. Sollte Power Platform Entscheidungen treffen, die ohne weiteres menschliches Zutun entstehen (sogenanntes „Automated Desicion Making" ADM) und sollten diese schwerwiegenden Auswirkungen haben (z. B. verschlechternde Umstufung in der Gehaltstabelle, (Nicht-)Gewähren von Boni, Versetzung, Kündigung) so ist das unzulässig (gemäß Artikel 22 DSGVO).

**Voraussetzung für die Nutzung von Power Automate und Power Apps sind folgende Punkte:**

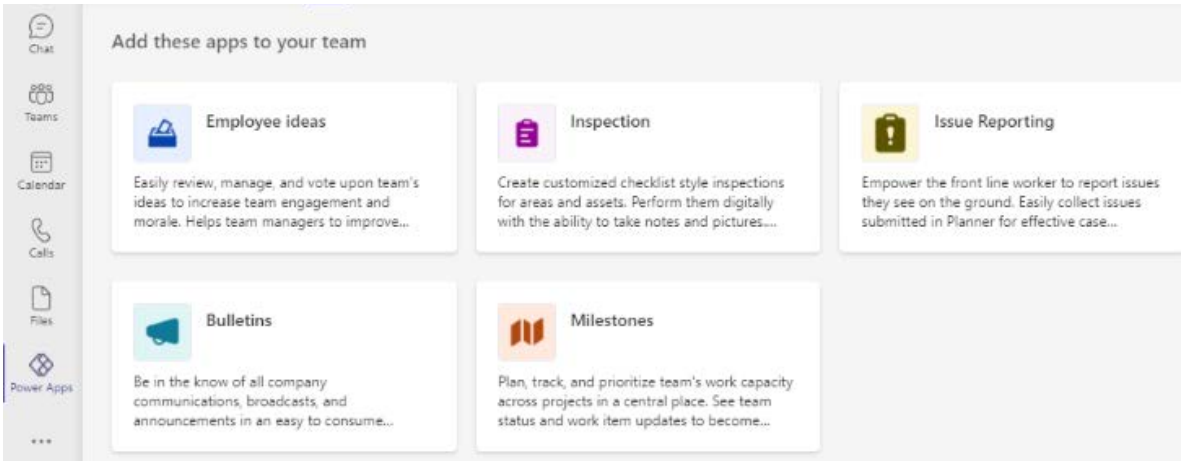
- Eine Lizenz zur Nutzung von Power Automate und Power App darf ausschließlich über das IT- Service Portal bestellt werden.
- Eine Liste mit Zugriffsberechtigten dem BR zugänglich machen.
- Eine Nutzung dieser Apps darf erst erfolgen, wenn an einer verpflichtenden Schulung mit besonderem Fokus auf Belange des Datenschutzes teilgenommen wurde.
- Die Anwendung darf nur zur Unterstützung einer konkreten Arbeitsaufgabe eingesetzt werden. Dieser Zweck ist zu dokumentieren.
- Eine Prüfung ist durchzuführen, ob ein Eintrag ins Verfahrensverzeichnis erforderlich ist und gegebenenfalls vorliegt.

**Power Apps** ermöglicht es auf einfachste Weise eigenständige Anwendungen für betriebsspezifische Bedürfnisse zu entwickeln. Mithilfe von Copilot kann so eine Anwendung ohne umfassendes Wissen in der Programmierung oder im Datenbankmanagement erstellt werden. Diese Vorgehensweise wird auch „vibe coding"genannt, also programmieren in Alltagssprache, nach Gefühl oder nach Stimmung.

Ein Anwendungsbeispiel wäre die Programmierung einer App für den Gutscheinverkauf im Betriebsrat. Mit Hilfe von Power Apps können eingehende Bestellungen und Bezahlungen erfasst sowie anschließend Emails automatisch versendet werden, sobald die bestellten Gutscheine eingetroffen sind. Weiters könnte die Gutscheinabgabe automatisch via QR Code erfolgen.
Power Apps können für eine Vertriebsanalyse, die IT-Auslastung oder das Verteilen von Arbeitsaufgaben verwendet werden. Es können öffentliche Daten hinzugezogen werden (z. B. wirtschaftliche Branchenanalysen). Es können Workflows für den Kundendienst erstellt werden, die automatisch Aufträge und benötigte Zeiten oder Standorte erfassen. Arbeitsabläufe zum Beantragen von Urlauben, könnten ebenso Gegenstand von Power Apps sein.

Bei der Entwicklung der betriebseigenen Anwendungen stellt nur die eigene Kreativität und der Zugang zu Daten eine Grenze dar – und hoffentlich auch das Arbeitsrecht.. Dass auch unerfahrene Benutzer:innen oder Personen ohne IT Kenntnisse Apps erstellen, kann zu gravierenden rechtlichen Problemen beim Beschäftigtendatenschutz sowie der Sicherheit führen. Insbesondere der Umgang mit besonders schutzwürdigen Daten stellt eine Problematik dar, wenn beispielsweise (versehentlich) personenbezogene Daten einem nicht dafür geeigneten Personenkreis zugänglich werden oder wenn die Sicherheitseinstellungen nicht korrekt konfiguriert sind. Im Idealfall ist der Betriebsrat bereits bei der Entwicklung des Anforderungskataloges einer Power-App-Anwendung mit an Bord und kann so sicherstellen, dass grundlegende Datenschutzrechte eingehalten werden.

**BEISPIEL FÜR „POWER" MIT „KÜNSTLICHER INTELLIGENZ"**



Bevor über Power BI automatisierte Berichte und Auswertungen erstellt werden, wird gemeinsam mit dem Betriebsrat festgelegt, ob Bedarf für derartige Anwendungen besteht und für welche Zwecke diese dienen sollen.

Es werden keine personenbezogenen Ergebnisse mit Power BI erstellt, sondern es umfassen diese immer Gruppen von zumindest zehn Personen. Es werden weiters keine personenbezogenen automatisierten Entscheidungen (ADM) getroffen.

Ergebnisse, Auswertungen und (grafisch aufbereitete) Ansichten von Power BI verbleiben innerhalb von Power BI, es erfolgt keine Übertragung in andere Formate oder Apps.

Die Erstellung von Berichten und Auswertungen in Power BI ist einem engen vorab geschulten und festgelegten Personenkreis gestattet.

Mit Power BI, Power Apps und Power Automate sollten ausschließlich eigens geschulte Beschäftigte arbeiten dürfen. Der Bedarf an zusätzlichen Analysen mit diesen Apps sollte vorab eingehend geprüft werden.

**Geregelt werden sollte:**

- Keine Downloads personenbezogener Beschäftigtendaten (z. B. in Excel-Sheets), weil damit weitere Bearbeitungen ermöglicht wären
- Einsicht des Betriebsrats im Admincenter vereinbaren, damit überprüft werden kann, wer welche Auswertungen macht bzw. ob die BV eingehalten wird
- nur in einem engen und geschulten Personenkreis verwenden (z. B. IT-Abteilung, Analyst:innen von Verkaufszahlen, ...)
- Zweck festlegen
- Verbot automatisierter Entscheidungen (ADM)
- Festlegen, ob die selbst definierten Apps verpflichtend durchzuführende Maßnahmen auslösen oder Vorschläge (z. B. bei Interaktion mit Kund:innen)
- Keine personenbezogenen Auswertungen (z. B. Auswertungen immer zu Gruppen von mindestens zehn Personen zusammenfassen)

## EXCHANGE

Exchange ist wohl der meistgenutzte E-Mail-Server. Auf Exchange werden E-Mails und Kalender verwaltet, Posteingang geregelt, E-Mail-Weiterleitungen eingestellt. Auf Exchange wird das firmenweite Adressbuch angelegt und Einsichtsrechte vergeben.

Sämtliche Kalender und E-Mails des Unternehmens können über Exchange synchronisiert werden und mit Hilfe der allfällig eingebundenen KI „voneinander lernen". Exchange „lernt" beispielsweise, dass während eines Flugs keine E-Mail empfangen werden, dass Besprechungen mit bestimmten Teilnehmenden länger dauern als geplant etc. Die Kommunikation der Nutzer:innen wird analysiert hinsichtlich der Prioritäten, der Lese- und Antwortgeschwindigkeit etc. Auf dieser Analyse aufbauend, können Regeln erstellt werden.

Regeln für den Umgang mit und vor allem zum Löschen von E-Mails zu erstellen, ist eine empfehlenswerte Vorgehensweise, um dem Prinzip der Datenminimierung gerecht zu werden.

Im Admincenter von Exchange kann für Postfächer, definiert werden, wie lange gelöschte Elemente aufbewahrt werden.

Es können Regeln eingerichtet werden, um E-Mails automatisch in ein anderes Postfach weiterzuleiten. Wenn weitergeleitet wird, bevor das Mail bei dem/der Empfänger:in landet, merkt es der/die Empfänger:in nicht und hat auch keine Chance, diese Weiterleitung zu entdecken. Ebenfalls können automatische Mailweiterleitungen an externe Adressen zu Datenschutz-Sicherheitslücken führen, weil Informationen ungeprüft auf externe Server übermittelt werden.

Über die Transportregeln (engl. „Mail flow rules“) und durch die Exchange Aministrator:innen kann überprüft werden, ob Weiterleitungen eingerichtet wurden.

Über den Exchange-Server kann eine Regel eingerichtet werden, damit sich Sicherungskopien nicht abändern oder löschen lassen ohne, dass die Nutzer:innen davon in Kenntnis gesetzt werden.

Falls auf Exchange relevante Sicherheitseinstellungen vorgenommen werden (z. B. Umgang mit Sicherungskopien, automatische Speicherung), sollten die Beschäftigten darüber informiert werden.

**In einer BV sollte insbesondere geregelt werden:**

- Berechtigungskonzept; Wer darf was?
- Welche Auswertungen werden standardisiert vorgenommen? Der Zugriff auf Auswertungen sollte jedenfalls wenigen Personen (z. B. in der IT-Abteilung) vorbehalten sein.
- Auf Backups (also ältere Versionen) sollten ausschließlich Administrator:innen zugreifen können
- Stehen die Regeln für Outlook [S. 41] und Teams [S. 43] mit denen von Exchange in Einklang?
- Sind „lernende“ Apps an Exchange angehängt; wenn ja, mit welchem Zweck?

## PURVIEW UND PURVIEW DEFENDER

Seit dem Update von Jänner 2023 tragen Safety-&-Security-Anwendungen von MS den Vornamen: Purview (Deutsch: Einfluss- oder Zuständigkeitsbereich). Microsoft Purview ist eine Plattform zu Datenverwaltung und Datensicherheit. Es umfasst mehrere Anwendungen zur Datensicherheit und zur Minimierung von Compliance Risiken, kurz: dem Datenmanagement.

### INHALT VON PURVIEW


Eine Anwendung davon ist der **Purview Defender** (Deutsch: Verteidiger). Dieser dient, wie der Name unschwer erkennen lässt, der Abwehr von Schad-Software (z. B. Trojaner, Viren, Würmer, offene Hintertüren). MS selbst gibt als Zweck „Erkennen von kompromittierten Nutzerkonten und unerwünschten Applikationen“ an. Die Zwecke der Überwachung sind insgesamt sehr weit gefasst; sie reichen von unangemessener Sprache über Beleidigungen und Offenlegung von vertraulichen Dokumenten gegenüber nicht-autorisierten Personen bis hin zu Aufdecken von (beabsichtigter und bevorstehender) Sabotage, Insider-Handel, Korruption und Geldwäsche.

Im Admin-Center von Purview (**Purview Compliance Portal**) werden die Regeln festgelegt, welche Aktivitäten als Bedrohung gelten und wann ein Alarm ausgelöst wird. Mittels Purview wird protokolliert, was vor und nach einem Vorfall, also einem Alarm, im gesamten Unternehmen passiert ist und auf Purview 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.

### ÜBERSICHT SECURITY-ANWENDUNGEN

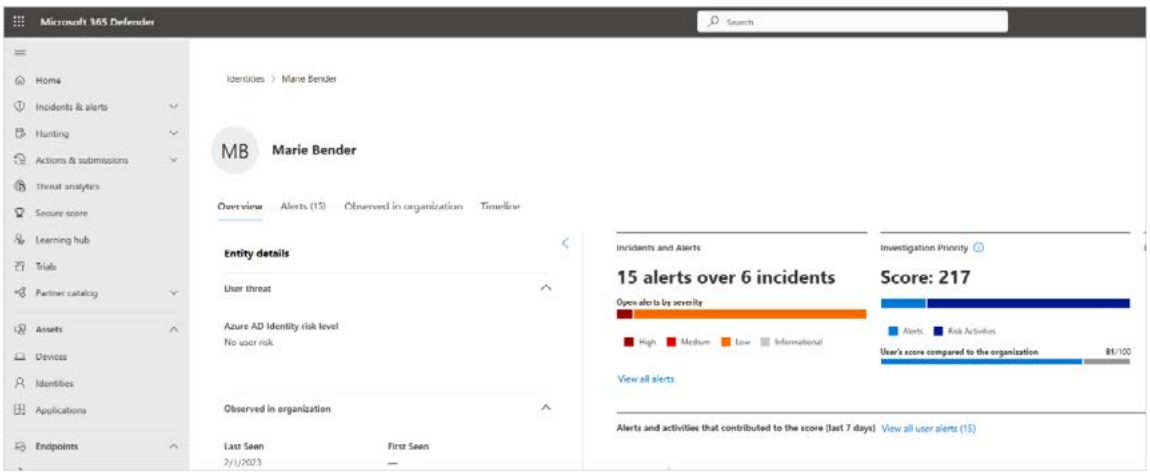

Für diese permanente Kontrolle werden die Inhalte von Emails, Chats, Dateien u.s.w. der Nutzer:innen klassifiziert und eingeordnet. Die Regeln (Englisch: communication compliance) können den vorgegebenen Standardeinstellungen folgen und/oder zusätzlich unternehmensintern definiert sein. Sie können mit einer Historie ausgestattet werden (trainable classifiers definition) sowie mit „Künstlicher Intelligenz" ergänzt werden, sodass eine durchaus extensive Überwachung die Folge sein kann. Beschäftigte werden aus Perspektive der Systemsicherheit oft als „Risiko" gesehen (siehe Abbildung unten).

Mit der Berechtigung „Microsoft Configuration Manager (ConfigMgr)" können Berichte darüber angesehen werden, ob Defender Sicherheitslücken bei mobilen Geräten gefunden hat (z. B. ob alle mobilen Geräte im Unternehmen die letzten Updates erhalten haben). Defender listet auf, von welchen Geräten ein besonders hohes Gefahrenpotential ausgeht und schlägt vor wie das Problem behoben werden kann (Englisch: „recommended Action").

Der Defender kann für Schulungen eingesetzt werden. Dabei werden Bedrohungsszenarien anhand der vorhandenen Daten entwickelt. Dazu schreibt beispielsweise Defender ein Programm, das einen Angriff simuliert. Öffnen Beschäftigte Anhänge von E-Mails, die Viren enthalten (Attachments von Phishing-Mails), verschickt Defender ein Fake-Mail an jene Beschäftigten, die als Risiko identifiziert wurden, damit diese ihre Reaktion verbessern können, sprich: die Anhänge nicht öffnen. So sollen die Nutzer:innen lernen, zukünftigen Schaden zu vermeiden. „Sensibilisierung und Training" nennt MS diese Vorgehensweise.

### RISIKOVERHALTEN EINZELNER

2. Wählen Sie die drei Punkte rechts neben dem Benutzer aus, und wählen Sie **Benutzerseite anzeigen** aus.



MS bietet „selbstlernende" Systeme, die im Voraus erkennen sollen, ob, wo und wodurch Gefahrenpotential besteht. Gehackte Anmeldedaten, betrügerische E-Mails, Schadsoftware und Ähnliches soll damit erkannt und abgewehrt werden.

**Für den Defender ist zu regeln:**

- Welche Aktivitätsprotokolle wie lange aufbewahrt werden
- Wer die Protokolle 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)
- 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
- biometrische Merkmale werden möglichst nur von einem eng begrenzten Personenkreis genutzt (z. B. jene mit Zugang zu streng vertraulichen Daten, Geschäftsgeheimnissen)

## E-DISCOVERY

Mit E-Discovery kann automatisiert, verdachtsunabhängig und revisionssicher jeder Sicherheitsvorfall gespeichert werden. Für Datenforensiker:innen, also jenen Fachleuten, die nach der Ursache von IT-Problemen suchen, ist das E-Discovery Gold wert, da damit sämtliche Kommunikationsverläufe und -inhalte nachvollzogen werden können. MS gibt Auskunft, dass E-Discovery für juristische Zwecke verwendet werden kann, da es Dateien vor (späteren) Manipulationen schützt, und nennt als Beispiel „Rechtsstreit". Der Zusatz zum Rechtsstreit „mit Mitarbeiten" fand sich 2022 noch auf der Webseite von MS, ist aber mittlerweile nicht mehr vorhanden. Auch ohne die explizite Erwähnung ist klar, dass eDiscovery sich zur Überwachung der Beschäftigten eignet.

Das E-Discovery kann dem simplen Wiederauffinden von Texten, Bildern, Chats, Tabellen, u.s.w. dienen. Zugangsberechtigte können aber auch mögliche Szenarien anlegen (sogenannte „Cases") und auf diese Weise nach eigens zusammengestellten Kriterien Durchsuchungen durchführen, die auch in die Privatsphäre der Beschäftigten hineinreichen. Wer Zutritt zum eDiscovery hat, kann darin Fälle anlegen, bei einem Gerichtsfall sämtliches Datenmaterial dazu auf „hold" stellen, also in der vorgefundenen Form aufbewahren und zum gegebenen Zeitpunkt (samt „Beifang") auswerten.

Für eine Zustimmung zum Einsatz des E-Discovery sollte sich der Betriebsrat gut überlegen, welche konkreten und begründeten Verdachtsfälle mit der Anwendung tatsächlich aufgeklärt werden könnten. Für ein schlichtes Auskunftsbegehren von Betroffenen wäre es ungeeignet, da es zu umfassend und unübersichtlich ist. Dafür gäbe es einfachere Mittel.

In den meisten Branchen und Betrieben sind die üblichen Archive und Speicherplätze ausreichend (z. B. Sharepoint [S. 67]), weshalb man den extra Behalte-Bereich des E-Discovery vermutlich nicht unbedingt benötigt.

**In einer BV sollte geregelt werden:**

- Zugriffsbeschränkungen (z. B. Forensiker:innen)
- eingeschränkte Zwecke (z. B. Gerichtsprozesse, schwere Sicherheitsattacken, Verbot einen Fall zur BR-Kommunikation anzulegen); Verbot der anlasslosen Nutzung
- Schweigepflicht für jene, die einen Fall mittels E-Discovery untersuchen (zumindest solange der Fall aufrecht ist)

- Informationspflicht an den Betriebsrat (soweit vom BR vertretene Personen von der Untersuchung betroffen sind). Recht des BR, sich allfällig angelegte „Cases" begründen und erläutern zu lassen

- Speicherdauer für die Ergebnisse festlegen

## COMPLIANCE PORTAL

Im **Compliance Portal** von Purview [S. 74] werden die Richtlinien für sämtliche MS 365-Apps festgelegt. Die Zugriffsberechtigungen werden entlang der hierarchischen Organisationsstruktur festgelegt, Berechtigungen für Anwendungen und Speicherorte werden vergeben, die Aufbewahrungsdauer für bestimmte Dateien wird geregelt (die sogenannten „Retention Policies"), Weiterleitungsrichtlinien werden fixiert u.s.w. Außerdem werden Benchmarks im Vergleich zum Sicherheitsrisiko anderer Firmen erstellt, forensische Berichte geliefert sowie Maßnahmen zur besseren Sicherheit empfohlen. Die Systemadministrator:innen können die Sicherheitsrichtlinien (Englisch: Security Policies) testen, analysieren, kontrollieren und (strenger) gestalten.

Ziel des Compliance Management ist es, Angriffe zu vermeiden, im Falle des Verlusts Dateien wiederherzustellen aber auch vorausschauend Bedrohungsszenarien zu erkennen und zu vermeiden oder zu simulieren und daraus Schulungen zu entwickeln.

MS 365 beinhaltet mehrere Möglichkeiten für Anmeldungen und damit verbundene Zutrittskontrollen. Um nur jene Personen mit den jeweiligen Apps arbeiten zu lassen, die das auch sollen, ist ein Zutrittsmanagement mittels Authentifizierung die Regel. Damit dabei nicht Privates mit Beruflichem vermischt wird, ist man in einem Betrieb übereingekommen, keine Merkmale mit Bezug zum Privatleben zu verwenden:

Generell gilt: Mitarbeiter nutzen ausschließlich ihre geschäftlichen Daten (Telefon, Mobilnummer, Emailadresse etc.) zur Anmeldung am geschäftlichen Microsoft Konto. Die Nutzung privater, mobiler Endgeräte zur Authentifizierung als auch die Eingabe von privaten Daten wird vom Arbeitgeber weder verlangt noch vorausgesetzt.

Der Zutritt zu einer App, also die Anmeldung der Nutzer:innen, besteht in der Regel aus mehreren eindeutigen und/oder einmaligen Identifizierungsmerkmalen (z. B. PIN, TAN und Passwort = **3-Faktor-Authentifizierung**). Ein sicheres Identitätsmanagement ist unbedingt erforderlich, damit Zugriffe von Unbefugten (z. B. von Unternehmensexternen) nicht passieren.

Das Programm von MS zur Verschlüsselung von Festplatten mobiler Geräte heißt „**bitlocker**".

„**Windows Hello**" bietet biometrische Zugriffskontrolle (z. B. Fingerprint, Iris-Scan), um eine eindeutige Authentifizierung zu ermöglichen. Biometrische Zugriffssperren werden vor allem beim Zugriff zu Cloud-Services von MS genutzt. So möchte MS Nutzer:innen automatisch informieren können, falls ihre Passwörter/PINs in falsche Hände geraten sollten.

**In einer BV sollte auf folgendes geachtet werden:**

- Zweck festlegen

- Speicherbeschränkung

- Zugriffsbeschränkungen (Welche Zugriffe dürfen mit welcher Art von Passwort erfolgen?)

- Rücksprache mit dem Betriebsrat, wenn neue Regeln erstellt werden

- Benachteiligungsverbot (z. B., wenn auf Simulationen zu Schulungszwecken unpassend reagiert wird)

- Festlegen, wie mit Biometrie umgegangen wird; keine Verwendung biometrischer Merkmale für eine Authentifizierung ODER biometrische Authentifizierung nur auf freiwilliger Basis, verschlüsselt und ohne Zugang für betriebliche Administrator:innen ODER ausschließlich für eine Personengruppe zulassen, die hochsicherheitsrelevante Tätigkeiten im Unternehmen ausübt

## ENTRA ID (VORMALS AZURE ACTIVE DIRECTORY)

Entra ID ist sozusagen der „Türsteher" für sämtliche Anwendungen. „Einmal hin, alles drin." erklärt es flott ein Systemadministrator.
Entra besteht aus mehreren Modulen (z. B. Domain Services, Permission Management, ID Protection etc.), die größtenteils der Systemsicherheit dienen.
Im Active Directory melden sich die Nutzer:innen an und identifizieren sich, wobei die IP-Adresse ebenso gespeichert wird, wie der Standort – so diese Funktion freigegeben wurde. In Entra ID wird bestimmt wer, wozu Zugriff hat. Es wird der Zugriff sämtlicher Geräte und Anwendungen reguliert.
Es gibt unterschiedlich hohe Sicherheitsvorkehrungen bei der Anmeldung. Je nachdem wie das Passwort gestaltet ist, ob ein TAN verwendet wird oder ob biometrische Merkmale wie Fingerprint und Augenirisscan (über die MS 365 App „Windows Hello") verwendet werden, ist der Zugang unterschiedlich sicher.

Der Umgang mit Informationen über den Standort wurde in einer Betriebsvereinbarung wie folgt festgelegt:

In der Theorie könnte auch auf den Standort zugegriffen werden. Da aber die Standortfunktion mittels der Main Policy deaktiviert ist, ist ein Zugriff durch die Systemadministration nicht möglich. Die bestehenden Funktionen wurden mit einer Grundeinstellung (der sogenannten „Main-Policy") vorgegeben (...) und können nur in Absprache mit der zentralen IT-Abteilung, dem BR und der zuständigen Führungskraft von der jeweils lokalen Systemadministration geändert werden.

Biometrische Merkmale zum Anmelden bei MS 365 zu verwenden, wird zwar als sehr sicher angesehen, weil sie nur einem Menschen auf der Welt zugeordnet werden können, ist meist aber übertrieben und somit nicht im Einklang mit der Rechtsprechung. Ein Urteil des Obersten Gerichtshofes besagt nämlich, dass der **Fingerscan zur Zeiterfassung eine überschießende Maßnahme** ist (OGH 9 ObA 109/06d) und eines der Datenschutzbehörde besagt, dass Handvenenscans zur Bestätigung der Zeiterfassung mangels ungültiger individueller Zustimmung ebenso unzulässig sind (DSB Entscheidung D124.2941). Umso überschießender wird es sein, ein solch heikles Merkmal für Vorgänge wie das Einloggen beispielsweise in Outlook zu verwenden.

Die Anmeldevorgänge werden aufgezeichnet und somit können Administrator:innen Verhaltensmuster ableiten (z. B. Wer meldet sich üblicherweise wann in welcher App an? Gibt es ein auffälliges Verhalten hinsichtlich der Anmeldezeitpunkte? Von welchem Standort melden sich Nutzer:innen meistens an? Für welche Dienste meldet sich wer besonders häufig an?).

**Zu regeln ist:**

- Berechtigungskonzept
- Für den Zugang zu besonders schützenswerten Daten eine 3-Faktor- Authentifizierung verwenden
- lesende Rolle für den Betriebsrat vereinbaren
- den Betriebsrat hinzuziehen, wenn personenbezogene Verdachtsfälle geprüft werden sollen

MS bietet die Rolle des „Privileged Identity Management" bei der zeitlich begrenzte für maximal acht Stunden Einsicht ermöglicht wird.

- Löschfristen für Überwachungsprotokolle festlegen
- Allfällige Verwendung privater Geräte und deren Zugang regeln

- biometrische Authentifizierung nur auf freiwilliger Basis, verschlüsselt und ohne Zugang für betriebliche Administrator:innen ODER: biometrische Authentifizierung via „Windows Hello“ ausschließlich für einen sicherheitsrelevanten Nutzer:innenkreis zulassen

## ENTRA ID PROTECTION

Diese Anwendung soll Sicherheitsrisiken erkennen, die durch (unberechtigte) Nutzer:innen ausgelöst werden, wie beispielsweise Anmeldeaktivitäten von nicht-registrierten Geräten, Versuche ein Passwort zu erraten, die Multi-Faktor-Authentifizierung zu umgehen, ungewöhnliche oder unmögliche Standorte von denen aus versucht wird auf interne Dateien zuzugreifen und vieles mehr.
Um solche sicherheitsbedenklichen Aktivitäten festzustellen, werden die Verbindungsdaten aus dem Entra ID [S. 78] ausgewertet und das Gefahrenpotential in hoch, mittel und niedrig eingestuft.

Eine Klassifizierung ist erforderlich, um beim Verlust von Daten oder dem unberechtigten Zugriff auf Daten feststellen zu können, wie groß der entstandene Schaden für das Unternehmen oder eine Person ist. Informationen rund um Bezahlvorgänge, Kreditkarten oder Geschäftsgeheimnisse werden wohl in den meisten Unternehmen dem höchsten Schutzniveau zugeteilt und ihre Zugriffe, allfällige Weitergabe etc. genauestens nachvollzogen. Es kann mittels Entra ID Protection herausgefunden werden, ob strafrechtlich relevante Ereignisse stattgefunden haben (z. B. Betrug, Spionage, Insider-Handel). Aber auch harmlosere oder unbeabsichtigte Compliance-Verstöße werden erfasst (z. B. Downloads von nicht-zertifizierten Webseiten). Der Betriebsrat sollte dafür Sorge tragen, dass anlasslose und flächendeckende Durchleuchtung aller Aktivitäten und Dateien nicht problematisch wird (z. B. weil BR-Korrespondenz in die falschen Hände gerät) indem klare Zugriffsrechte und Verantwortlichkeiten festgelegt sind (z. B. in einer BV).

Werden Dateien als Hochrisiko eingestuft und betreffen sie außerdem personenbezogene Daten von Beschäftigten, sollte deren Interpretation und Ableitung von Maßnahmen mit dem Betriebsrat gemeinsam durchgeführt werden.

Ereignisse mit den Risikostufen „Mittel“ und „Hoch“ werden so lange gespeichert, bis sie behoben oder verworfen werden. Alle Vorfälle mit der Risikostufe „Niedrig“ sowie die Benutzenden werden sechs Monate lang gespeichert, bis sie automatisch als veraltet markiert werden.

**In einer Betriebsvereinbarung sollte geregelt sein:**

- Strenge Zugriffsregelungen
- Zweckbeschränkung auf konkrete Vorfälle mit schwerwiegenden Folgen (z. B. Schadensbeurteilung bei juristischen Auseinandersetzungen, Angriffe auf die IT-Sicherheit)
- Klares Prozedere, welche Maßnahmen im Falle eines entdeckten „hohen Risikos“ getroffen werden (z. B. Zugriff sperren, Freigabe blockieren und wie der Betriebsrat einzubinden ist
- Beschäftigte deren Identität nicht mehr sicher ist (z. B. deren Account gehackt wurde), sollen betriebsintern anonym bleiben

## DATA LOSS PREVENTION (DLP)

Auf Deutsch würde diese Anwendung etwa „Datenverlust-Schadensabwehr“ heißen oder präziser aber komplizierter: „Schutz gegen den unerwünschten schadenverursachenden Abfluss von Daten“. DLP dient vereinfacht gesagt dem Auffinden verloren gegangener Daten. Mit DLP kann festgestellt werden, ob Dateien (illegal) entfernt, verschoben, weitergeleitet wurden. Die Vorgaben, was als auffällige oder gefährliche Aktivität gilt, werden in DLP erstellt (z. B. Kreditkartennummern dürfen nicht per E-Mail versendet werden). Es kann ein Schwellenwert definiert werden, wann eine Warnung ausgeschickt wird (z. B., wenn Dokumente zu Steuern und Abgaben nach vier Jahren statt wie vorgeschrieben nach sieben Jahren gelöscht werden). Der Hintergrund für DLP ist eine Klassifikation der Dateien. Es wird je nach Betrieb unterschiedlich sein, was als „streng vertraulich“ oder „öffentlich

zugänglich" klassifiziert wird. Ohne ein solches „Label", also eine Plankette, zu jeder Datei, bringt ein DLP nicht viel, da nicht herausgefunden werden kann, ob der Verlust von Dateien eine Gefahr darstellt. Im DLP kann festgelegt werden, welche Maßnahmen bei Dateiverlust welcher Vertraulichkeitsstufe folgt (z. B. bei Löschen eines streng vertraulichen Dokuments, wird umgehend geprüft ob dazu eine Berechtigung vorhanden ist und falls nicht, kann das Dokument nicht gelöscht werden).

Warnungen dürfen allerdings nicht die Arbeit des Betriebsrats beschränken (z. B. wenn als „vertraulich" gekennzeichnete Dokumente des Betriebsrats mit Warnungen versehen werden, wäre die Betriebsratsarbeit behindert).

**Die wichtigsten Punkte sind entsprechend jenen zu anderen Sicherheitsanwendungen in einer Betriebsvereinbarung zu regeln:**

- Zugriff strikt auf IT-Abteilung beschränken
- Regelung und Information an die Beschäftigten, was im Falle des Auftauchens eines Sicherheitsrisikos, was im Falle eines entdeckten Angriffs bzw. eines Verdachts auf einen solchen zu machen ist
- Regeln für „die Prüfung im Anlassfall (z. B. Keywords" mit dem BR gemeinsam erstellen, Überwachung vertraulicher Kommunikation im Beisein des BR)
- Speicherfristen für festgestellte „Risiken"
- Betroffene Arbeitnehmer:innen nicht bloßstellen sondern möglichst Anonymität zusichern

## INTUNE

Diese App ist dazu da, alle in einem Unternehmen registrierten mobilen Geräte wie Smartphones, Laptops, IPads und Ähnliche zu verwalten und sicherheitstechnisch zu überprüfen. Alle Geräte sollen übereinstimmend, im Gleichklang mit den betrieblichen (Sicherheits-)Vorgaben, auf Englisch also „in tune", funktionieren. Intune untersucht die vorhandenen mobilen Geräte beispielsweise auf Viren, ermöglicht den Fernzugriff und kann die Sperre von Accounts veranlassen. Über Intune können Geräte geortet werden. Intune ist die Anwendung in MS 365 zum Mobile Device Management (MDM), also der Verwaltung mobiler Geräte.

Intune bietet – ebenso wie andere Security-Tools – verschiedene Berichte über die Aktivitäten auf mobilen Geräten. Darunter ein Bericht der Echtzeit-Daten umfasst und für Administrator:innen und Kolleg:innen am Helpdesk nützlich sein kann, um sofort Maßnahmen einzuleiten (z. B. Löschen sensibler Daten wenn ein Gerät gestohlen wurde). Der historische Bericht bietet Muster und Trends über einen längeren Zeitraum. Diese Berichte sind für IT-Managementebene und Administrator:innen nützlich, sollten aber nur für ausgewählte Anlassfälle unter Beteiligung des BR personenbezogen ausgelesen werden. Auch der „spezialisierte Bericht", der die Verwendung von Rohdaten zur Erstellung benutzerdefinierter Berichte ermöglicht, sollte nur unter BR-Information und Beteiligung möglich sein.

**In einer BV regeln:**

- Zugriffsmöglichkeiten auf IT-Abteilung beschränken und festlegen, wann der Betriebsrat informiert und wann er hinzugezogen werden muss
- Die Beschäftigten informieren, bevor auf ihnen zugeordneten Geräten Manipulationen vorgenommen werden (z. B. Zugriff, Löschung, Sperre, Zurücksetzen etc.)
- Vom Einbinden privater Geräte wird eher abgeraten
- Die Standorterfassung kann über das Admincenter deaktiviert werden


## SENTINEL

Microsoft Sentinel liegt auf MS-eigenen Servern (cloudbasiert), ist für jede Unternehmensgröße und Datengröße anpassbar (skalierbar), dient dem Sicherheitsmanagement (SIEM – Security Information and Event Management) kann automatisiert reagieren (SOAR – Security Orchestration Automated Response) und schützt das Unternehmen vor Cyberangriffen. Es ist nicht Teil des Software-Pakets von Microsoft 365, sondern Teil der Azure-Plattform, kann aber eigens gekauft werden. Dass es in der Broschüre dennoch erwähnt wird, ist der Häufigkeit in Unternehmen und der Wichtigkeit von Sicherheitstools geschuldet.

Sentinel sammelt und untersucht Informationen aus verschiedenen Quellen im Unternehmen, um mögliche Gefahren frühzeitig zu erkennen und darauf zu reagieren. Dabei nutzt es künstliche Intelligenz und maschinelles Lernen, um große Datenmengen zu analysieren und komplexe Bedrohungsmuster zu erkennen.

Sentinel verbessert die IT-Sicherheit, aber verarbeitet gleichzeitig Mitarbeiter:innendaten, die mitunter eher der Privatsphäre der Beschäftigen zuzurechnen sind. Daher ist es entscheidend, den Datenschutz und die Rechte der Beschäftigten zu wahren. Eine sorgfältig ausgearbeitete Betriebsvereinbarung ist empfehlenswert, um den Einsatz von Sentinel zu regeln und somit für IT-Sicherheit sorgen, ohne die Privatsphäre der Beschäftigten zu gefährden.

Sentinel eignet sich hauptsächlich für größere Unternehmen, da spezialisiertes IT-Personal erforderlich und kontinuierliche Wartung notwendig ist, was für kleinere Betriebe herausfordernd sein kann. Zudem basiert das Preismodell auf dem zu sichernden Datenvolumen, was für größere Unternehmen mit entsprechenden Budgets tragbar ist. Preislich günstiger ist Sentinel für Unternehmen, die bereits Microsoft-Lösungen nutzen.

© iStock

# NACHWORT

Bevor diese Broschüre gedruckt vorliegt, wird es zu einzelnen Anwendungen und Funktionen schon wieder Neuigkeiten geben. Die Angebotspalette in der Welt von MS365 wandelt sich wesentlich rascher als es in anderen Universen üblich war und ist. Die gelungene Betriebsratsmitsprache geht daher Hand in Hand damit, wie es gelingt mit der Geschwindigkeit Schritt zu halten und die geeigneten Routinen zu finden.

Es braucht wohl keine Kristallkugel um vorauszusagen, dass User:innen sehr bald und sehr vermehrt auf „selbstlernende" Features bei MS 365 treffen werden. Für Spannung beim nächsten Update der Broschüre ist gesorgt. Eine andere Prognose sei noch hinzugefügt: Im Gegensatz zu den zahlreichen Updates und Verbesserungen von MS 365, die für permanente Veränderung und so manche Überraschungen sorgen, wird die Pflicht, zu MS 365 eine Betriebsvereinbarung abzuschließen, bestehen bleiben.

Dieser Text soll dabei helfen, den Überblick zu bewahren und die beste zum Unternehmen passende Betriebsvereinbarung auszuhandeln, um Beschäftigte vor zu starker (offener oder versteckter) Überwachung zu schützen.

An der Entstehung dieser Publikation der Gewerkschaft GPA waren mehr Menschen beteiligt als im Impressum ersichtlich sind. Spezieller Dank geht an die Interessengemeinschaft IT der Gewerkschaft GPA für ihre Erfahrungsberichte; insbesondere an **Franz Schäfer**, der Open Source Alternativen zu MS zusammengetragen hat sowie **Julian Sommer-Schmelzenbarth**, der für die Beantwortung kniffliger Fragen im Admin-Bereich bereitgestanden ist. Außerdem gilt **Asim Dadan** besonderer Dank, der mit seiner Erfahrung aus der IT-Security die Liste der aktuellen und meistverwendeten Apps überprüft hat.

Aus der Gewerkschaft GPA hat der Informatiker **Matthias Rausch** sein Open-Source-Wissen einfließen lassen und **Isabel Koberwein** hat mit ihrer Expertise aus dem Arbeitnehmer:innen-Schutz den Text mit den Gesundheitsaspekten bereichert. Und der letzte aber umso wichtigere Dank geht an **Dagmara Sperska**, die ihr korrekturlesendes Adlerauge über den gesamten Text geworfen hat.

# ARBEITSMATERIAL

## OPEN-SOURCE ALTERNATIVEN ZU MICROSOFT 365

Ein Problem bei MS Anwendungen ist, dass sie schlicht und einfach deshalb verwendet werden, weil sie verfügbar sind und weil ein Großteil der Nutzer:innen meint, mit ihnen umgehen zu können, weil die Nutzeroberfläche bereits vertraut scheint. Vielfach werden Office-Programme aber für Aufgaben eingesetzt für die sie nicht gut geeignet sind (z. B. Word für umfangreiche Dokumente mit zahlreichen unterschiedlichen Formatierungen). „Wenn dein einziges Werkzeug ein Hammer ist, sieht alles aus wie ein Nagel“ ("If your only tool is a hammer then everything looks like a nail") könnte man dazu sagen.
Läuft der Großteil der IT-Infrastruktur im Betrieb über MS365 sind die Anwendungen gut miteinander verbunden (in der IT spricht man auch von guter „Integration“). Läuft der Großteil der IT-Infrastruktur im Betrieb über MS365 wird dadurch gleichzeitig ein hohes Abhängigkeitsverhältnis geschaffen, einerseits eine Abhängigkeit von MS und dessen Eigentümer:innen und gleichzeitig von den USA und deren Datenschutzregime beziehungsweise deren Regierung. Im Fall der Sanktionen der USA gegen den Iran wurde beispielsweise der Export von Microsoft Produkten verboten. Im Falle eines Handelskrieges könnten auch Microsoft Produkte betroffen sein, Daten abfließen oder der Zugriff auf sie verwehrt werden, was zu erheblichem wirtschaftlichem Schaden führen könnte.
Das Abhängigkeitsverhältnis wenn sämtliche Software von Microsoft bezogen wird, kann für viele Betriebe letztlich teurer werden (zum Beispiel bei Preiserhöhungen) als eine eigene Infrastruktur zu betreiben.
Eine unternehmenseigene IT-Infrastruktur ist natürlich mit Aufwand verbunden. Für größere Firmen sollte das aber kein Problem sein und kleinere können auf gehostete, also von einem externen Dienstleister zur Verfügung gestellte Versionen dieser Programme zurückgreifen.
Es muss also nicht immer MS sein. Es gibt Alternativen und viele davon sind Open Source, basieren also auf einem Code, der einsehbar und veränderbar ist.

Diese Zusammenstellung ist weder abschließend noch beständig. Wie jedes digitale Werkzeug unterliegen die hier dargestellten Alternativen technischen Änderungen sowie Änderungen von Besitzverhältnissen und damit der Firmenphilosophie. Jeder Betrieb muss daher die IT-Infrastruktur selbst so auswählen, dass sie zu dem gegebenen Rahmenbedingungen, der Unternehmenskultur, den Beschäftigten und ihrem IT-Knowhow, dem Kerngeschäft, dem Budget etc., passt.

### BÜRO-SOFTWARE/OFFICE-PROGRAMME:

Ein geeignetes Werkzeug für online Zusammenarbeit mit Kolleg:innen ist das weit verbreitete **LibreOffice**. LibreOffice ist eine freie Open-Source Software, das heißt, der Programmcode ist im Internet offengelegt. LibreOffice wurde von der Document Foundation entwickelte und umfasst eine Textverarbeitung (ähnlich Word), eine Tabellenkalkulation (ähnlich Excel), Präsentationssoftware (ähnlich PowerPoint), ein Vektorgrafikprogramm (ähnlich Visio),

ein Datenbankverwaltungssystem (vergleichbar mit MS Access) und einen mathematischen Formeleditor. Es gibt eine Version die online als Server betrieben werden kann, was einige Firmen wiederum als Service anbieten z. B. **Collabora Online**.
In Deutschland wird derzeit die Bedeutung und das Potential von Open-Source-Software für die digitale Souveränität thematisiert – vorwiegend im staatlichen und öffentlichen Bereich. So hat die schleswig-holsteinische Regierung bereits dem Wechsel auf LibreOffice als Standard für Bürosoftware für rund 25.000 IT-Arbeitsplätzen zugestimmt.

## ONLINE ZUSAMMENARBEIT / DOKUMENTENAUSTAUSCH/ COLLABORATION:

Ein einfaches Werkzeug, um gemeinsam an Texten zu arbeiten ist **Etherpad**. Jeder eingegebene Buchstabe wird sofort allen anderen Bearbeiter:innen ersichtlich. Etherpad bietet öffentliche Instanzen an, womit also gratis gearbeitet werden kann, was für eine Testversion optimal ist. Es gibt etwa 290 "Plugins", also „Stöpsel“, mit denen weitere Software für verschiedenste Zwecke angedockt werden kann (z. B. für die Bearbeitung von Tabellen oder einen Audio-Video-Chat). Etherpad wurde 2009 von Google gekauft, die Codes sind aber weiterhin öffentlich.
Für (gemeinsames) Präsentieren, Erstellen von Videos, eignet sich die ursprünglich von einem ungarisch-schwedischen Künstler-Architekten-IT-Team entwickelte Software **Prezi**, deren Zentrale mittlerweile in San Francisco, USA, beheimatet ist. Wer Powerpoint und Sway von MS ersetzen möchte, für die ist Prezi (derzeit) öffentlich gratis zu haben, oder zum internen Firmengebrauch im monatlichen Abonnement.
Während die bekannteren Anbieter zur online Kollaboration wie Padlet, Sli.do oder Webex ihren Code nicht öffentlich machen, sind weitere Open Source Angebote für jene, die nicht mit MS Teams arbeiten möchten, **claper**, **mindwendel** (für Abstimmen, Quiz und Ähnliches im Bildungsbereich genutzt) oder **spacedeck**.

## DOKUMENTENABLAGE/ WISSENSDATENBANKEN/ WIKIS:

Oft braucht man eine ganze Menge von Dokumenten, die übersichtlich abgelegt werden sollen und die miteinander inhaltlich verbunden sind, aufeinander Bezug nehmen (referenzieren). Dafür sind Wikis ein gutes Werkzeug. Die **MediaWiki** ist jene Software die für die weltweite Wikipedia eingesetzt wird. Es gibt noch weitere wie **Wiki.js**, **DokuWiki** oder **BookStack**. Auch hier gilt: Es gibt Firmen die gehostete Instanzen, also von ihnen betreute Server, von OpenSource Wikis anbieten. Man kann diese auch auf einem firmeneigenen Server betreuen, also „hosten“.

## KURZNACHRICHTENDIENSTE/ MESSENGER /CHAT:

Gerade im Bereich von Chats gibt es sehr viele Applikationen. Die bekannteste von Datenschützer:innen empfohlene ist **Signal**, das auch zum (Video-)telefonieren genutzt werden kann. Weitere Chat-Services sind z. B. **element**, **matrix** oder **mattermost**, die von eigenen Dienstleistern betrieben werden. Die meisten beinhalten die Möglichkeit zur Video-Telefonie und Matrix eine Schnittstelle mit den Konferenz-Tool **jitsi**.

## VIDEO CONFERENCING / BILD-TELEFONIE:

**jitsi** ist eine Videokonferenz-Software. Man kann sie gratis benutzen oder im eigenen Unternehmen installieren und betreiben. Ehrlicherweise muss dazu gesagt werden, dass jitsi bei längeren Gesprächen mit mehreren Teilnehmer:innen technische Schwächen hat.

Gut geeignet ist die Plattform **BigBlueButton** für die online Zusammenarbeit (z. B. auf dem Whiteboard), das Teilen von Materialien (z. B. mit KI-unterstützten „Smart Slides“) und Videotelefonie (z. B. in eigenen „Klassenräumen“)

geeignet. Content- und Lernmanagement sind inkludiert. Es wird gerne für den Unterricht verwendet. Der Vorteil ist, dass BigBlueButton auch bei Videokonferenzen mit einer größeren Anzahl an Teilnehmenden stabil läuft.

**UMFRAGEN:**

Statt mit MS Forms können Befragungen mittels **LamaPoll** durchgeführt werden, einer Open-Source-Software aus Deutschland, die für nicht kommerzielle Zwecke für kurze Zeit kostenfrei genutzt werden kann. Für regelmäßige Umfragen gibt es kostenpflichtige, je nach Anzahl der Befragten unterschiedliche Abonnements.

**E-MAIL:**

Statt MS Exchange gibt es andere zahlreiche E-Mail-Provider, also Anbieter oder Dienstleister, die auf offenen Standards basieren (IMAP = Internet Message Access Protocol, Netzwerkprotokoll, das ein Netzwerkdateisystem für E-Mails bereitstellt). Diese **IMAP-Server** werden beispielsweise von **cyrus** oder **curier** als Open-Source betrieben und spielen gut mit den vielen freien E-Mail-Anbietern wie **postfix** oder **exim** zusammen.
Die Systeme sind leicht zu installieren und brauchen deutlich weniger Ressourcen als Microsoft-Exchange. Wer allerdings selbständig Mail Systeme hosten will, muss mit einigem Aufwand rechnen, um die SPAM-Filterung, also das Aussieben unerwünschter oder mit Viren verseuchter Nachrichten, in den Griff zu bekommen.

**KALENDER:**

Ein Kalender muss nicht immer mit E-Mail verknüpft sein. Viele Menschen haben z. B. ihre E-Mail bei einem Provider und nutzen einen anderen für ihre Termine (z. B. Mozilla Calendar). **Mozilla Thunderbird** ist ein kostenloses Open-Source-Programm, das E-Mail, Kalender, Instant-Massaging sowie Adressbücher zusammen enthält. Es bietet eine übersichtliche Benutzeroberfläche, kann eine große Menge an einzelnen E-Mail-Accounts verwalten, ermöglicht Anpassung an andere Systeme. Die Kalenderfunktion trägt den Namen „**Lightning**“ und bietet wichtige Sicherheitsfeatures (z. B. OpenPGP-Verschlüsselung, Phishing-Schutz, Spamfilter). Der Anbieter Mozilla ist bekannt dafür, dass Wert auf Datenschutz gelegt wird.

**SERVER:**

Server die man selbst betreiben kann und auf denen diverse Funktionen gemeinsam betreut werden können sind z. B. **Owncloud** oder **Nextcloud**. Diese Cloudserver können nicht nur zum Speichern und Organisieren von Dateien genutzt werden, sondern auch um zahlreiche Funktionen erweitert werden (z. B. Office-Anwendungen zur gemeinsamen Dokumentenbearbeitung, Terminkalender, Kontaktverwaltung, E-Mail-Client, und vieles mehr). Mittlerweile können diese Open-Source-Cloudserver durch eigene Verschlüsselungen abgesichert werden. Es werden Desktop- und Handy-Apps angeboten, die die lokalen Daten kontinuierlich mit der Cloud synchronisieren.

Um **alle Dienste**, Anwendungen, Services und Funktionen **aus einer Hand** nutzten zu können, wird in der öffentlichen Verwaltung von Deutschland **openDesk** entwickelt. Das Zentrum für Digitale Souveränität (ZenDiS) koordiniert im Auftrag der deutschen Bundesregierung dieses Vorhaben. Ende Mai 2024 erhielten zwei Anbieter den Zuschlag (B1 und StackIT) und bauen nun OpenOffice zu einer europäischen cloudbasierten Anwendung aus, um die Abhängigkeit von Microsoft in der öffentlichen Verwaltung zu reduzieren. openDesk beinhaltet viele der oben genannten Open-Source Lösungen (Nextcloud, Collabora, Element und OX). Es bleibt zu hoffen, dass open Desk längerfristig auch in anderen europäischen Ländern und auch Privatpersonen oder Unternehmen zur Verfügung stehen wird.

# CHECKLISTE: (BASIS-) BETRIEBSVEREINBARUNG ZU MS 365

- ☐ **Rechtsgrundlage** §§ 96 und 96a ArbVG (ev. in Verbindung mit Artikel 88 DSGVO)
- ☐ **Überblick** über aktivierte, im Betrieb verwendete Apps/Anwendungen von MS 365 (siehe Beiheft)
- ☐ Klarstellung, dass einzelne Tools, die personenbezogene AN-Daten verarbeiten, in **Zusatz-Betriebsvereinbarungen** geregelt werden
- ☐ **Verwendungszweck** für die jeweiligen Apps festlegen
- ☐ **Berechtigungskonzept**
- ☐ **Löschfristen** nach dem S.T.O.P.-Prinzip [S. 22]
- ☐ **Schulungen** vereinbaren und unterscheiden zwischen verpflichtenden und optionalen
- ☐ **Ansprechpartner:innen** im Unternehmen für MS 365 ernennen (z. B. externe Expertin oder externer Experte, Keyuser:innen, „Champions" etc. [S. 34])
- ☐ **Privatnutzung** regeln und zulassen solange sie die betrieblichen Abläufe nicht stört und keine Schäden verursacht
- ☐ **Freiwilligkeit** so weit als möglich festlegen (z. B. OneDrive [S. 60]) aber zumindest bei Freigabe persönlicher Informationen (Foto, Status etc.)
- ☐ **Mitbestimmung** des Betriebsrates im Prozess der Einführung und Adaptierung regeln
- ☐ Empfehlung: Einrichtung einer **Arbeitsgruppe** MS 365, die sich einmal pro Quartal trifft
- ☐ Anzeigen von **Auswertungen** grundsätzlich einschränken (insbes. Viva [S. 52])
- ☐ **Maßnahmen**, die auf BV-widrigen Auswertungen und Kontrollen beruhen, sind unwirksam bzw. müssen zurückgenommen werden, ebenso allfällige Benachteiligungen
- ☐ **Kontrolle** von Einzelpersonen ausschließlich anlassbezogen (bei nachgewiesenem Fehlverhalten) im Beisein eines Betriebsratsmitglieds
- ☐ Heimliches/verdecktes Vorgehen gegen einzelne Arbeithmer:innen
- ☐ Erstellen von **Profilen** zur Leistungsbeurteilung unterbinden (z. B. Ranking, Boni etc.)
- ☐ Umgang mit **Updates** regeln (Testlaufe, Testuser:innen)
- ☐ Regelmäßige **Evaluierung** (vgl. § 4 ASchG [S. 23])

# CHECKLISTE: MS 365 IM EINKLANG MIT DSGVO?

**Die wichtigsten Fragen um festzustellen, ob MS 365 in Übereinstimmung mit der DSGVO verwendet wird, sind:**

- ☐ Wurde die **Rechenschaftspflicht** eingehalten (vgl. Art 5 Abs 2 DSGVO), d. h. sind die Verwendungsvorgänge von MS 365 dokumentiert?

- ☐ Wurde **Datensparsamkeit** praktiziert (vgl. Art 5 Abs 1 c DSGVO)?

- ☐ Wurden die Betroffenen über die Datenverwendungen in MS 365 **informiert** (Transparenzgebot, Informationspflicht zu verwendeten Daten, Verwendungszweck, Empfängerkreisen, Verantwortlichen, Löschfristen vgl. Art 13 DSGVO)?

- ☐ Wurde eine **Datenschutzfolgenabschätzung** vorgenommen (vgl. Art 35 DSGVO)?
    - ○ Wurde eine Risikobewertung bzw. eine Schwellenwertanalyse für AN vorgenommen?
    - ○ Wurden die Betroffenen/der **Betriebsrat** eingebunden? (gemäß Art. 36 Abs 9 DSGVO)
    - ○ Wurden Abhilfe geschaffen gegen allfällig bestehende Risiken?
    - ○ Ist der/die betriebliche Datenschutzbeauftragte eingebunden gewesen?

- ☐ Haben die Betroffenen **eingewilligt** (vgl. Art 6 DSGVO) – falls es sich um freiwillige Features handelt?
    - ○ Ist die Zustimmung zur Verwendung von MS 365-Apps an die (Weiter-)Beschäftigung oder andere das Arbeitsverhältnis betreffende Faktoren gekoppelt? → wenn ja, wäre die Einwilligung nicht freiwillig und könnte außerdem dem „Koppelungsverbot" (Art. 7 Abs 4 DSGVO) widersprechen.

- ☐ Wurde die Privatsphäre der Arbeitnehmer:innen durch **technische Einstellungen** geschützt (Art. 25 DSGVO)?
    - ○ Sind die Einstellungen und Nutzungsbedingungen so festgelegt, dass den Arbeitnehmer:innen ein möglichst großer Spielraum zur freiwilligen und diskriminierungsfreien Verwendung einzelner Apps bleibt (z. B. Ausschalten des Status, Ausschluss von Aufzeichnung, Archivierung etc.).

- ☐ Sind die MS 365-Anwendungen ins **Verarbeitungsverzeichnis** eingetragen (vgl. Art. 30 DSGVO)?

- ☐ Gibt es **Auftragsverarbeiterverträge** (AVV) mit Microsoft, die über die im Internet angebotenen Standardverträge hinausreichen?
    - ○ Wenn ja: Sind darin Datenübertragungen an MS enthalten? Wenn ja: Welche?
    - ○ Wenn ja: Gibt es eine Rechtsgrundlage für diese Datenübermittlung in Dritt-Staaten?

mitgliedwerden.gpa.at

MEINE GEWERKSCHAFT