DIE WUNDERBARE WELT VON MICROSOFT

und wie der Betriebsrat sie mitgestalten kann

Aus der Broschürenserie **GUTE ARBEIT!**
Gewerkschaft GPA – Abteilung Arbeit & Technik

gpa MEINE GEWERKSCHAFT

„Die neue Online-Welt der Microsoft-Apps ist vielfältig und dynamisch, erscheint dabei aber teilweise unübersichtlich bis chaotisch“

Max Thomsen (Technologieberater, in „Computer und Arbeit“ 05/2021)

„Bei vielen Anwendungen weißt du als Nutzer gar nicht mehr, wo du bist – ob du überhaupt noch auf Microsoft 365 bist.“

(ein Nutzer am 13.9.2022)

„Eine ausufernde Erwartung an Verantwortliche ist praxisfern und blockiert technischen Fortschritt.“

(Stellungnahme von Microsoft Deutschland am 25.11.2022)

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

Stand: Februar 2023

GUTE ARBEIT!

AUTORIN

© Edgar Ketzer

Mag.ª Clara Fritsch

ist Soziologin und arbeitet in der Abteilung Arbeit & Technik der Gewerkschaft GPA. Ihr Arbeitsschwerpunkt beinhaltet die Themen Kontrolle am Arbeitsplatz, Beschäftigten-Datenschutz, Whistleblowing, Personalentwicklungssysteme sowie algorithmische Entscheidungsfindung. Dazu schult und berät sie Betriebsrät:innen und begutachtet Betriebsvereinbarungen.

VORWORT

© Daniel Novotny

Der „Alleskönner“ unter den Software-Giganten bietet neben einem weithin bekannten Betriebssystem namens „Windows“ auch mehr oder weniger bekannte Software zur Textbearbeitung, Tabellenkalkulation, Dokumentenverwaltung, Telefonie, Spracherkennung, Kooperation, Präsentation, Suchfunktionen, Selbstoptimierungsprogramme, Projektmanagement, Gerätemanagement, Zugriffsmanagement, Passwortschutz, Sicherheits-Richtlinien und einiges mehr – ob privat oder im Betrieb, in der Schule, in der Fabrik oder im Krankenhaus. Software von Microsoft ist von Arbeitsplätzen nicht mehr wegzudenken. Microsoft bewältigt immer mehr Arbeitsaufgaben und wird immer leistungsstärker.

Microsoft bietet einige seiner Anwendungen im Paket an. Seit 2011 steht dieses Softwarepaket Firmen und seit 2013 Privatpersonen „in der Cloud“, also auf Microsofteigenen Servern, zur Verfügung und wird nun „Microsoft 365“ (MS 365) genannt. Gar viele Fragen stellen sich im Zusammenhang damit: Wer kann die höchst umfangreiche Software-Palette noch überblicken? Wer hat das notwendige Knowhow, um die unzähligen Apps, Features und Einstellungen von MS 365 kritisch zu begutachten? Gelten in der Cloud andere Regeln? Wie ist was womit und zu welchem Zweck verknüpft? Warum sollte man sich überhaupt mit einem einzigen Unternehmen so ausführlich beschäftigen? Warum ändert sich ständig etwas bei Microsoft 365? Braucht es ein eigenes Wörterbuch, um MS 365 zu verstehen? Und was geht das die Gewerkschaft an?

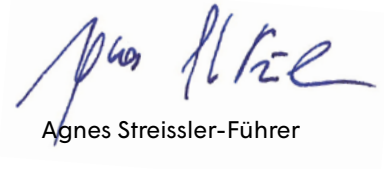
Spricht man von Konzernen, die mit Internet-Dienstleistungen groß geworden sind, fällt schnell die Abkürzung „GAFA“ (die Abkürzung steht für Google/Alphabet, Apple, Facebook und Amazon). Immer wieder liest und hört man von deren (Skandal-)Geschichten. Auffällig unauffällig ist dagegen Microsoft in diesem Akronym und in der medialen Berichterstattung. Als solider Hersteller von Betriebssystemen in den 1980er Jahren bekannt geworden, zählt der Konzern weder zu den neuen noch zu den skandalträchtigen Tech-Giganten. In Sachen Büro-Software nimmt Microsoft eine Monopolstellung ein.

VORWORT

Diese Marktmacht von Microsoft hat dazu geführt, dass sich auch die Gewerkschaft näher mit dem Konzern und seinen Produkten auseinandersetzen muss. Der Bedarf nach mehr Information rund um Microsoft 365 zeigt sich in den zunehmenden Anfragen der Betriebsrätinnen und Betriebsräte zu dem äußerst schnelllebigen, flexiblen und breiten Angebot. Es braucht mehr Hilfestellung für die Interessenvertretung bei der betrieblichen Verwendung von Microsoft-Produkten. Es war an der Zeit für die Gewerkschaft GPA, das vorliegende Werk in Angriff zu nehmen – wissend, dass es nie vollständig, geschweige denn abgeschlossen sein wird. (Nicht thematisiert werden in der Broschüre beispielsweise Produkte aus dem Microsoft-Universum, wie der Browser „Edge" oder die Virtual-Reality-Brille „HoloLense".)

Diese Broschüre zum betrieblichen Einsatz von Microsoft 365 spiegelt mit ihren vielen Querverweisen und den eng miteinander verzahnten Kapiteln die Welt von MS 365 wider. Einige Kapitel geben einen Ein- und Überblick zu MS 365 und andere beschäftigten sich ausführlich mit den arbeits- und datenschutzrechtlichen Aspekten von MS 365. Die nach unserer Beratungserfahrung in der Gewerkschaft GPA am meisten eingesetzten sowie die heikelsten Apps von MS 365 werden im zweiten Teil dargestellt, wobei im Abschluss zu den einzelnen Apps immer die wichtigsten in einer Betriebsvereinbarung zu regelnden Punkte zusammengefasst sind. Die grauen Kästchen enthalten – je nach Symbol – Tipps zur Verwendung von MS 365 beziehungsweise Zitate aus Betriebsvereinbarungen. 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

INHALT

 Besonderheiten in der Welt von MS 365

 Zitate aus bestehenden (Muster-)Betriebsvereinbarungen zu MS 365

 Wichtige Hinweise zur Verwendung von MS 365

DIE WELT VON MICROSOFT

WAS IST DAS BESONDERE AN MS 365?

Der Konzern Microsoft (MS) ist derzeit **Marktführer** in Unternehmens-Software und Betriebssystem. Microsoft hat in den letzten Jahren besonders durch den Ausbau von Programmpaketen wie Office [S. 38] oder Outlook [S. 39] sowie durch sein Betriebssystem Windows einen Monopolstatus erreicht. Besonders seit dem Corona-bedingten Lockdown im März 2020 und dem damit einhergehenden Arbeiten im Home-Office sind die (unter anderem auch lizenzfreien, also gratis verfügbaren) Microsoft-Produkte zum ortsungebundenen Arbeiten, wie beispielsweise Teams [S. 42], deutlich häufiger im Einsatz.

MS 365 (ehemals „Office 365“) ist seit Oktober 2010 auf dem Markt und umfasst ein ausgenommen **breites Angebot.** MS 365 enthält eine Menge einzelner Anwendungen, sogenannte Apps, mit einer noch größeren Menge an Funktionalitäten (z. B. zur Planung, Logistik, Kommunikation, Kollaboration, Security, Mobilität, Device-Management, Personalmanagement u.v.m.). Die meisten Ressourcen steckt Microsoft derzeit in den Ausbau der Kollaborations-Software Teams [S. 44] sowie in die Entwicklung der Spracherkennung und -steuerung [S. 58].

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 kollektiver Ebene, als auch für das Management auf höchster Ebene sind Anwendungen in MS 365 inkludiert. Es gibt Software, die für ein gesamtes Unternehmen von Bedeutung ist (z. B. die „Steuerungszentrale“ Azure Active Directory der „Türsteher“ MS Defender als Sicherheits-Software [S. 64] etc.). Für das Management auf der Ebene von Gruppen, Bereichen, Abteilungen oder Niederlassungen hat MS 365 auch einiges im Angebot (z. B. die Plattform Sharepoint [S. 60], die Plattform zur Personalverwaltung MS Dynamics [S. 53], das Compliance Center [S. 66], wo allgemeine Richtlinien eingerichtet werden u.s.w.) und für die einzelnen Nutzer:innen gibt es jede Menge Apps, sowohl zur Koordination mit anderen (z. B. Teams, Outlook etc.) als auch zur Organisation der eigenen Arbeit (z. B. OneDrive).

Ein wesentliches Merkmal von MS 365 ist, dass diese Ebenen und Anwendungen alle über den sogenannten „Graph“ [S. 49] miteinander verbunden sind.

Die einzelnen Anwendungen werden **permanent „verbessert“**, ausgebaut, untereinander kombiniert, sprich: verändert. Apps werden anderen Unternehmen abgekauft (z. B. 2011 kaufte MS Skype, 2013 die Handysparte von Nokia um sie 2018 an Foxconn zu verkaufen; 2018 wurde GitHub gekauft u.s.w.) oder neu erfunden und in die bestehenden Apps integriert (z. B. wurde im Jänner 2022 Viva [S. 50] hinzugefügt). Anwendungen werden mit anderen zusammengespielt oder auch nicht mehr weiterentwickelt und „versickern“ (z. B. wird Skype seit 2021 nicht mehr serviciert).

So wurde auch an einer Künstlichen Intelligenz zur Gesichts- und Emotionserkennung auf Fotos, einschließlich Angaben zum ungefähren Alter und Geschlecht,

geforscht, diese aber aufgrund mangelnder Wissenschaftlichkeit im Juni 2022 wieder eingestellt – für ausgewählte Kundinnen und Kunden soll ein Ableger davon („Seeing AI" für Blinde und Sehbeeinträchtigte) allerdings weiter zur Verfügung stehen.[1]

Immer wieder werden Apps, also Programme, von MS 365 umbenannt (z. B. führen einige der Security-Apps nun den Namen „Purview").

Manche Funktionen tauchen unter andere Namen wieder auf (z. B. die Auswertungsmöglichkeiten von „WorkplaceAnalytics" in „Viva Insights").

MS bietet auch Funktionen, die in mehreren Apps im Einsatz sind. Manche Features sind quer über verschiedene Ebenen aktiv (z. B. Standort, Präsenzstatus, Sprachsteuerung). Sie sind jedoch auf keinen Update- und Release-Plänen und auch auf keiner „Road-Map" namentlich ausgewiesen. Man könnte sie als **„Meta-Anwendungen"** bezeichnen. Beispielsweise kann die Spracherkennung in einem einfachen 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 Kalenderaufgaben mit der MS Sprachassistentin „Cortana".

Außerdem beinhaltet MS 365 Möglichkeiten zur **Einbindung externer** Apps/Programme/Anwendungen/Module. So ist beispielsweise seit dem Erwerb der Plattform LinkedIn durch MS ein Button im Mailprogramm Outlook vorhanden, um die Profile auf Outlook und LinkedIn miteinander abzugleichen. Derartige Erweiterungen machen die Sache nicht übersichtlicher.

Und eines ist sicher: **MS 365 ist immer in Bewegung.**

MS 365 kann auf unterschiedliche Art betrieben werden. MS 365 kann auf firmeneigenen Servern laufen (Bezeichnung dafür lautet „on premise") oder die Apps werden aus der **Cloud** heruntergeladen oder gleich

1 https://www.derstandard.at/story/2000136778322/zu-gefaehrlich-microsoft-stoppt-oeffentlichen-zugang-zu-ki-die-emotionen (Letzter Zugriff: 14.3.2023)

sämtlich dort betrieben. MS 365 kann also verwendet werden, ohne dass firmenintern Systemadministratorinnen oder Systemadministratoren tätig werden oder firmeneigene Server erforderlich sind. Bei der Cloud-Variante von MS 365 findet die Datenverarbeitung auf Servern von MS statt, wobei die Kundinnen oder Kunden/Nutzer:innen/Unternehmen nur auf ihre eigenen Datenbestände Zugriff haben (sollten). Die MS Server sind verstreut über unterschiedliche Standorte und 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. Das führte insbesondere aufgrund des In-Kraft-Tretens der Europäischen Datenschutzgrundverordnung (DSGVO) zu massiver Kritik, da Speicherorte auch außerhalb der EU liegen sowie Transparenzgebot und Rechenschaftspflichten nur schwer zu erfüllen sind. 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 an".[2]

Bei MS Cloud-Anwendungen wird die verwendete Software nicht mehr im Unternehmen installiert, gewartet, aktualisiert, repariert, ausgetauscht, ergänzt etc. Für die meisten Unternehmen liegt darin ein großer Vorteil, da zeit- und ressourcenintensive Aufgaben wegfallen. Personal, Speicherkapazitäten, IT-Knowhow, Bug-Fixes (also das Beheben von Software-Fehlern), Updates (also Aktualisierungen und Erweiterungen der Software), das alles stellt MS zur Verfügung. Auch die **Verfügbarkeit** dürfte bei diesem Cloud-Dienst verlässlicher und durchschnittlich besser gegeben sein als bei den meisten firmenintern betriebenen Systemen. Gleiches gilt für die technische **Sicherheit** und Gefahrenabwehr (engl. „safety and security"), in die MS Kapazitäten investiert, die einer einzelnen Kundein oder einem einzelnen Kunden im Regelfall nicht zur Verfügung stehen.
Mit dem vom MS gebotenen Komfort fallen hingegen eigene Gestaltungsmöglichkeiten weg. Software, die vom Hersteller verwaltet wird, enthält vom Standard abweichende Möglichkeiten nur dann, wenn dafür gezahlt wird – zum Beispiel mit einer Premium-Lizenz.

Werden Anwendungen von MS genutzt, hat das den Nebeneffekt, dass sämtliche Nutzungsdaten (auch Metadaten oder Telemetriedaten genannt) bei MS landen. MS kann damit Vergleiche anstellen, „Benchmarks" erzeugen (also Schwellenwerte ab denen etwas als „gut" oder „schlecht" bewertet wird), alte Anwendungen „verbessern" und den Bedarf an neuen Anwendungsmöglichkeiten analysieren. Dieser Datenschatz und die darauf basierenden Innovationen sind es, die MS groß gemacht haben.

Die Vorteile liegen auf der Hand.

Die gute Seite von MS 365

- MS funktioniert weitgehend stabil, weil sich die über den gesamten Erdball verteilten Serverfarmen bei Problemen gegenseitig ersetzen können.
- MS bietet orts- und zeitunabhängiges Arbeiten, weil die Server rund um die Uhr und von jedem Standort aus erreichbar sind und permanent serviciert werden.
- Raubkopien und unbefugte Lizenznutzungen sind kaum problematisch, weil alles auf MS-eigenen Rechnern betrieben wird und vieles ohnehin gratis angeboten wird.
- Kontinuierliche Zahlungen in Form von Lizenzgebühren sind für Unternehmen besser planbar als bei einmaligem Kauf (neuer) Software.
- Es existieren „maßgeschneiderte" Lösungen, weil die Nutzung minutiös aufgezeichnet wird und der genutzte Leistungsumfang bekannt ist, woraus diese passgenauen Lösungen abgeleitet werden.

2 https://news.microsoft.com/de-de/unsere-antwort-an-europa-microsoft-ermoeglicht-speicherung-und-verarbeitung-von-daten-ausschliesslich-in-der-eu/ (Letzter Zugriff: 14.3.2023)

INTERPRETATION VON BESCHÄFTIGTEN-DATEN – WAS MACHT MS 365?

MS 365 bietet eine riesige Menge an Anwendungen und Einstellungen. Alle Anwendungen sind im Hintergrund miteinander über Graph [S. 49] verknüpft. Jede Anwendung kreiert – egal ob von den Nutzer:innen gewollt oder nicht – im Hintergrund Verbindungs- und Verhaltensdaten (sogenannte Metadaten oder Telemetriedaten). Dabei handelt es sich nicht nur um die Nutzungsdaten Einzelner (z. B. deren persönliche Einstellungen, individuelle Nutzungshäufigkeit, Nutzungszeiten etc.), sondern auch um die Beziehungen der einzelnen Nutzer:innen untereinander (z. B. Reaktionsgeschwindigkeit anhand von Durchschnittswerten, 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, Teams) oder die Nutzung mit einem Zeitstempel versehen (z. B. Office, Teams) 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 – technisch ist das nicht anders möglich.

Hier muss die dadurch mögliche Kontrolle der Arbeitnehmer:innen über organisatorische Maßnahmen unterbunden werden. Die Interpretation dieser Daten darf nicht zu Lasten der Beschäftigten gehen. Idealerweise werden diese Statusinformationen überhaupt nicht weiter interpretiert, außer als das, was sie sind: eine Auskunft darüber, ob jemand gerade angibt, beschäftigt zu sein oder verfügbar.

MS 365 in der Cloud ist permanent online und übermittelt damit permanent Daten an Microsoft, die zur Verbesserung der Services oder zu deren Stabilität und Sicherheit erforderlich sind. Die Geschäftsführung bzw. die IT-Abteilung könnte (über sogenannte „man-in-the-middle-proxy") auf die übermittelten Daten zugreifen. Der Verwendungszweck dieser Daten „zur Verbesserung der Produkte und Dienstleistungen" kann und wird von MS umfassend interpretiert.

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

- versendet ein/e Teilnehmer:in während eines Meetings E-Mails über Outlook [S. 39], führt das zu Auffälligkeiten (sog. „Findings") und wird als Meeting mit geringer Qualität („Low Quality Meeting") interpretiert.

- haben Nutzer:innen Terminkollisionen in ihren Kalendern (z. B., weil ein abgesagter Termin nicht gelöscht wurde), geht man in der MS-Logik von „abgelenkten Teilnehmern" aus.

- sind einem Termin keine weiteren Teilnehmer:innen zugeordnet, die aus den MS 365 Kontakten bekannt sind, wird der Termin als potenzielle „Fokuszeit" gewertet. (Das ist Zeit, die MS den Nutzer:innen vorschlägt, um ungestört und konzentriert arbeiten zu können.) Um die beste Fokuszeit herauszufiltern, wird ausgewertet, wie „aktiv" jemand in einer MS 365-Anwendung gearbeitet hat. Dazu werden vermutlich Aktivitäten gemessen und mit der „Verweildauer" in einer bestimmten App in Beziehung gesetzt. So schlägt MS z. B. auch Termine als potenzielle „Fokuszeiten" vor, bei denen es sich tatsächlich um ein Webinar oder einen Arzttermin handelt.

- Outlook [S. 39] nimmt eine durchschnittlich benötigte Zeit für das Verfassen eines E-Mails an. Weicht jemand von dieser Annahme ab, wird dies als „ineffizient" bewertet. Es wird dabei keinerlei Rücksicht darauf genommen, ob es sich um ein kurzes E-Mail mit dem Inhalt „Hallo, da bin ich" handelt oder um die Stellungnahme zu einem komplexen Sachverhalt.

- Bestehen viele Interaktionen (z. B. gemeinsame Termine, gemeinsam bearbeitete Listen, geteilte OneDrives etc.) mit anderen Personen aus den Kontakten, wird dieser Umstand positiv beurteilt. Kolleginnen oder Kollegen mit hohem „Vernetzungsgrad" werden als „erfolgreicher" bewertet – wer kein ausgedehntes Netzwerk hat, gilt als weniger erfolgreich. In der beruflichen Praxis könnte eine hohe Zahl an Interaktionen aber theoretisch ihren Ursprung in Unselbstständigkeit haben. Die quantitative Menge an E-Mails sagt nicht unbedingt etwas über deren Qualität aus; viele unklar formulierte E-Mails sind nicht zwangsläufig besser als ein verständliches.

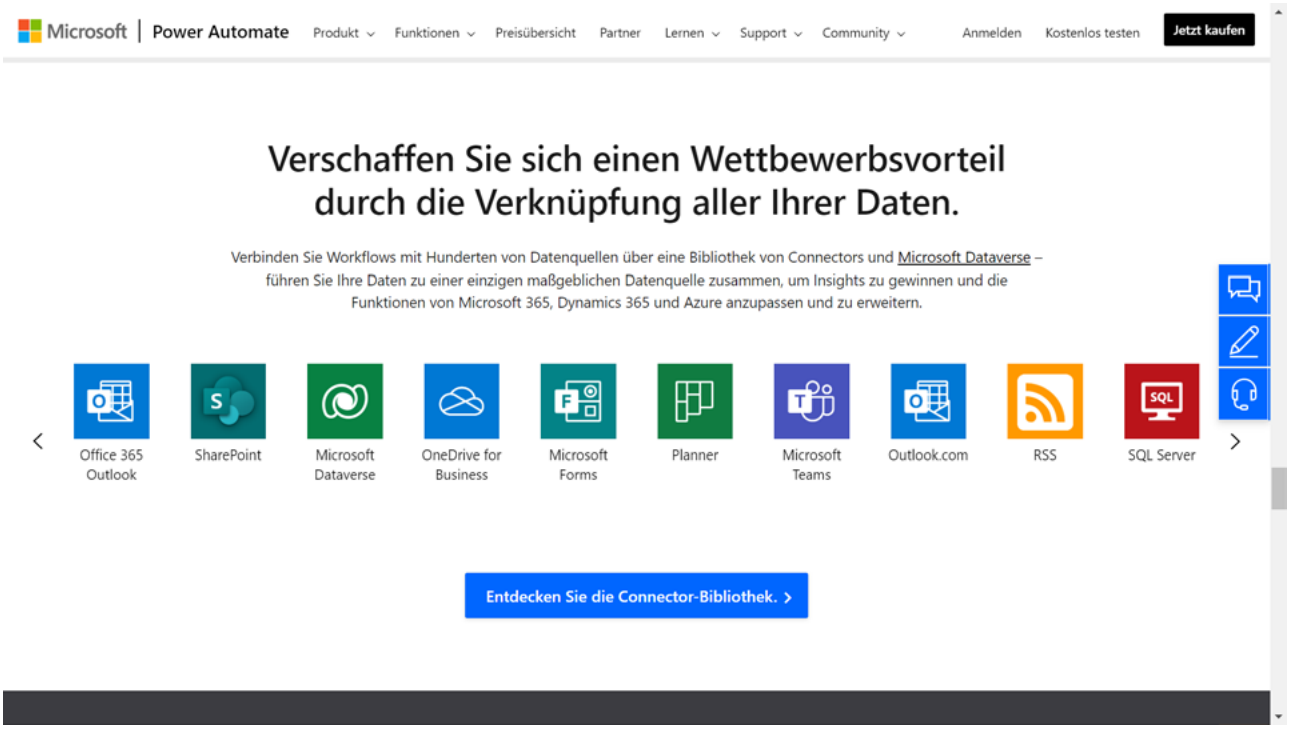
- Die Benutzeranmeldung über „Azure Active Directory“ [S. 66] schätzt den Standort ein, an dem man sich gerade befindet. Das führt bei mobiler Arbeit dazu, dass der Aufenthalt im Zug-WLAN der Deutschen Bahn tendenziell eher dem Standort Berlin zugeordnet wird, mobile Datennutzung generell jedoch eher dem Standort Frankfurt am Main.

- „Viva Insight“ [S. 50] berechnet, wann die individuell besten Zeitfenster für „well-being“ bestehen, wobei die genauen Berechnungsgrundlagen weitgehend im Dunkeln bleiben. Viva Insight verrät Tipps wie „deaktivieren sie Arbeit außerhalb der Arbeitszeit“. In der MS 365-Welt ist aber alles, was außerhalb der eigenen MS-Anwendungen geschieht, keine „Arbeit“ – es kann ja nicht gemessen werden.

MS 365 kann nur jene (Verbindungs-)Daten verarbeiten, die mit MS-eigenen oder mit MS verknüpften Apps erstellt werden. 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-Kanälen (z. B. mastodon), leitet eine Videokonferenz, die nicht von MS stammt (z. B. zoom) und nicht mit MS 365 verlinkt ist bzw. eingebunden wurde, 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. MS geht davon aus, dass sämtliche Arbeitsaktivitäten innerhalb der Galaxis von MS ablaufen.

MS 365 errechnet also Zusammenhänge, die nicht unbedingt sinnvoll sind und trifft damit Aussagen über – mitunter auch zukünftiges – Sozialverhalten, zeiteffizientes Verhalten, oder finanzielle Effekte. Nachdem die Rechenvorgänge im Hintergrund aber nicht offengelegt werden, ist nicht ersichtlich, ob die Grundannahmen sinnvoll sind. Genauso unklar bleibt, ob ethische Grundprinzipien mit einfließen (z. B., dass Entscheidungen aufgrund von maschinellen Berechnungen jederzeit rückholbar sein müssen). Ebenso unklar ist, ob die Berechnungen wissenschaftliche Grundprinzipien der Mathematik und Statistik einhalten. Ohne die Berechnungsgrundlagen zu kennen, sind sämtliche Empfehlungen von MS 365 also 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 berechtigt.

VERMEINTLICHER VORSPRUNG DURCH VERKNÜPFUNG VON DATEN



HANDLUNGS-MÖGLICHKEITEN DES BETRIEBSRATES

Aus dem **Arbeitsverfassungsgesetz (ArbVG),** dem **Arbeitnehmer:innenschutzgesetz (ASchG)** und der **Europäischen Datenschutzgrundverordnung (DSGVO)** ergeben sich für den Betriebsrat viele Möglichkeiten, wie sie oder er sich bei der Gestaltung von MS 365 einbringen kann.

- Betriebsrätinnen oder Betriebsräte können sich darauf berufen, dass sie die Einhaltung von **gesetzlichen Vorgaben überwachen** müssen (z. B., wenn sie oder er z. B. Einsicht in Auswertungen von MS Dynamics nehmen wollen). Um seinen Kontrollpflichten nachkommen zu können, hat der Betriebsrat (BR) verschiedene Möglichkeiten. Beispielsweise kann sie oder er eine eigene Rolle, also eine eigene Leseberechtigung, für MS 365 einfordern [S. 27]. Der BR kann eine MS 365-Datenschutzgruppe ins Leben rufen [S. 33] und regelmäßige Informationstreffen initiieren. Der BR kann fixe Informationsabläufe einfordern, die bei Änderungen von MS 365 einzuhalten sind.

- Sie oder er kann eine **Anhörung** verlangen, bei der sie oder er Vorschläge zur Gestaltung von Apps macht (z. B. Präsenzstatus ausschalten).

- 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 Checkliste der MS 365 Apps [S. 73] und die Checkliste „Was in einer (Basis-)Betriebsvereinbarung zu regeln ist" [S. 71]).

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

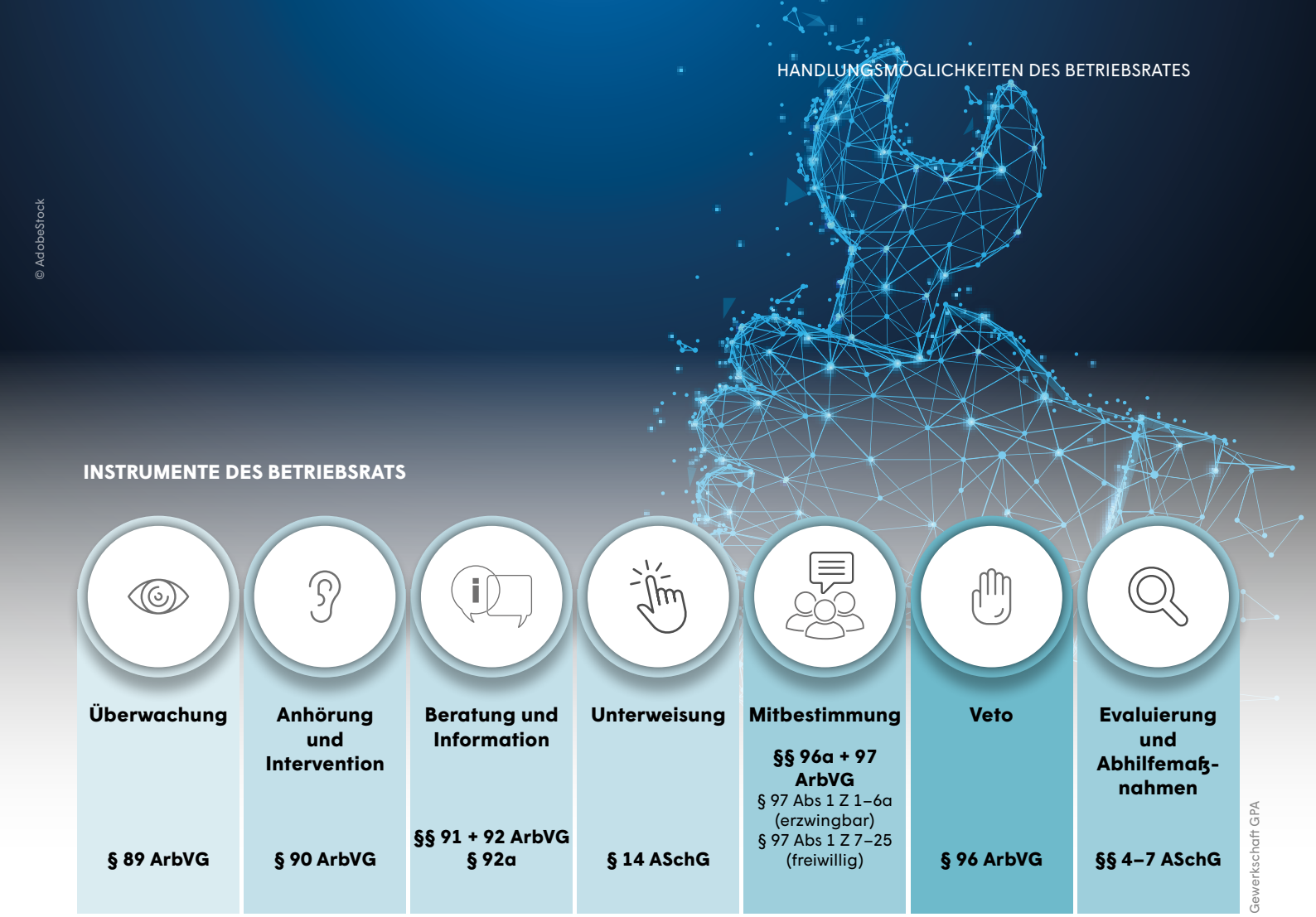
- Sie oder er kann und soll **Einsicht** verlangen in die Ergebnisse der **Evaluierung** und der **Abhilfemaßnahmen** von gesundheitlichen Gefahren (z. B. psychische Belastung durch steigende Kontrollmöglichkeiten über den Aktivitätsstatus, Stress durch Überzahl an Kommunikationskanälen, Überforderung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

- Der Betriebsrat muss eine **Betriebsvereinbarung** durchsetzen.

Es stehen dem Betriebsrat also einige rechtliche Bestimmungen zur Verfügung, mit denen die Interessen der Belegschaft vertreten und durchgesetzt werden können.

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 Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, 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 eine Betriebsvereinbarung erforderlich, denn (fast) jede Software ist dazu geeignet, Arbeitnehmer:innen zu kontrollieren. Angesichts der geradezu lückenlosen Aufzeichnung des persönlichen Nutzungsverhaltens durch MS 365, ist anzunehmen, dass eine Betriebsvereinbarung gemäß § 96 Abs 1 Z 3 ArbVG abzuschließen ist.

Die Begriffe „Kontrollmaßnahme" (bzw. „technische Systeme zur Kontrolle der Arbeitnehmer") 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 also aus, damit ein System zustimmungspflichtig ist. Somit werden die vielfältigen Datensammlungen von MS 365 sicher miterfasst sein, da sie allein durch ihre Vielzahl eine weitrechende Kontrolle ermöglichen.

Von einem Berühren der **Menschenwürde** ist jedenfalls dann auszugehen, 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 in der Regel sehr viele Arbeitsprozesse erfasst sind, kann eine weitgehend lückenlose Aufzeichnung der Tätigkeiten von Arbeitnehmer:innen erfolgen.
Soll nun beurteilt werden, ob die Menschenwürde tatsächlich berührt ist, ob also ein Betriebsvereinbarungspflicht gegeben ist, muss auch beachtet werden, was konkret im Betrieb im Einsatz ist.[3] Der 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.

3 OGH 14.7.2022, 9 ObA 60/22x. Verhandlungsgegenstand war die BV-Pflicht zu einem System, das Bewegungsprofile ermöglicht. Der OGH hat den Fall zurückgewiesen.

Das ArbVG beinhaltet eine weitere Grundlage 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 Arbeitnehmern 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 sich das Gesetz auch auf bereits bestehende Systeme. Die Erweiterung, die Abänderung, die Verknüpfung 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 Mitbestimmungsvorschrift 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, Sozialversicherungsnummer; 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 und deren personenbezogene Daten von MS 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 Wege 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 die 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.

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** bedarf (ebenso wie jeder andere Verarbeitungsvorgang) einer Rechtsgrundlage, in diesem Fall ist das ein 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 Rechtslage[4] angepasst und MS nennt sie nun „**Microsoft Products and Services Data Protection Addendum (DPA)"**.[5] Mittels dieser Verträge soll die Datenverwendung von personenbezogenen Daten bei MS in den USA legalisiert werden.

Dass MS Daten in den USA verarbeitet war bereits länger 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)[6], die die alten Klauseln ersetzen und die Übermittlung personenbezogener Daten zwischen der EU und Dritt-Ländern ohne Angemessenheitsbeschluss erleichtern sollen.
Wie der EuGH in seinem Urteil schreibt, kann jedoch, auch mit diesen Standarddatenschutzklauseln nicht schon von vornherein davon ausgegangen werden, dass den Grundsätzen der DSGVO genüge getan ist. Der oder die Übermittler:in hat jedenfalls im Einzelfall (mit Unterstützung der Datenschutzbehörden) zu prüfen, ob im Zielstaat ein angemessenes Datenschutzniveau gewährleistet ist. Die Datenübermittlung in die USA ist damit nun erheblich erschwert und mit einem rechtlichen Risiko behaftet.

Zwischen EU und USA wurde vereinbart, dass man einen Angemessenheitsbeschluss für den Datentransfer in die USA ausverhandeln möchte. Eine „Executive Order" von Präsident Joe Biden hat dieses Anliegen im Dezember 2022 (wieder einmal) bekräftigt. Es bleibt abzuwarten, ob diese – noch abzuschließende – Vereinbarung im Endeffekt halten wird. Bei den vorherigen Abkommen „Safe Harbor" und „Privacy Shield" war das Ablaufdatum schneller erreicht als gedacht.
Die meisten Server für europäische Microsoft-Kundinnen oder -Kunden stehen mittlerweile in Europa. Dennoch kann Microsoft nicht gänzlich ausschließen, dass personenbezogene Daten der Kundinnen und Kunden und Nutzer:innen, also auch der Arbeitnehmer:innen, in den USA verarbeitet 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. Eine Zusammenfassung der Anfragen zur Freigabe von Inhaltsdaten und deren Freigabe publiziert der Konzern in seinem halbjährlichen "Law Enforcement Request Report".[7] In diesem Report steht, dass im ersten Halbjahr 2022 zu 219 Accounts aus Österreich Anfragen gestellt wurden, aber keine personenbezogenen Inhaltsdaten offengelegt wurden.

Datenschutzfolgenabschätzung (DSFA)

Wird eine DSFA erstellt, wird vorab in einer so genannten **„Schwellenwertanalyse"** eingeschätzt, 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.

4 EuGH 16.07.2020, C-311/18; https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=37280 (Letzter Zugriff: 14.3.2023)
5 https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA (Letzter Zugriff: 14.3.2023)
6 https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_de (Letzter Zugriff: 14.3.2023)
7 https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report (Letzter Zugriff: 14.3.2023)

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. Rechtlich verantwortlich für die Durchführung der DSFA ist dennoch 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" zum Einsatz kommen, ist ebenso eine DSFA erforderlich. Künstliche Intelligenz bietet MS 365 beispielsweise bei Authentifizierung über Sprache oder bei der Textanalyse, die „mitschwingende Gefühle" erkennt. In Zukunft wird MS in dem Bereich noch stärker investieren, beispielsweise bei der Firma „OpenAI" und deren „ChatGPT", der derzeit führenden KI bei Bild- und Texterstellung.
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.

Keine Betriebsvereinbarung kann aber datenschutzrechtliche Mängel 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 nicht unternehmensspezifisch definiert und somit nicht unmittelbar an den Zweck der Datenverarbeitung gebunden werden. Gemäß DSGVO dürfen personenbezogene Daten jedoch nur so lange aufbewahrt werden, als sie einem legitimen Zweck dienen. Verwendet ein Unternehmen MS 365 ist es in vielen Fällen an die von MS vordefinierten Aufbewahrungsfristen gebunden.

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, mitunter „selbstlernende" Systeme, die personenbezogene Daten der Nutzer:innen verwenden (z. B. Bewertung von Telemetrie-Daten in Delve [S. 47], Empfehlungen in Viva [S. 50]).

MS bemüht sich laufend um Verbesserungen. So wurde beispielsweise das Tool „Diagnosedatenanzeige" erstellt, mittels dem Nutzer:innen wenigstens prüfen können, welche Telemetrie-Daten an MS weitergegeben werden.

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. 50]). Die Erstellung von Profilen erfolgt, ohne dass die Informationspflichten an die Betroffenen, also die Nutzer:innen, eingehalten werden. Diese Information müsste den Zweck, die Empfänger 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. Karriereschritte 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). 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 überhaupt dazu berufen ist, ihren Einsatz konkret einzuschätzen und man damit nicht sprichwörtlich den „Bock zum Gärtner" macht.

Es wurden und werden immer wieder **Sicherheitslücken** festgestellt. Beispielsweise finden Datenübermittlungen in die USA statt, vor allem bei Security-Apps. Es wurden Daten unterschiedlicher Unternehmen (Clients) auf denselben Servern gespeichert und nur unzureichend voneinander getrennt. Im März 2021 wurde bekannt, dass der Exchange Server mehrerer deutscher Bundesbehörden gehackt worden war. 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 wohl keine echte Freiwilligkeit geben. Die Freiwilligkeit ist aber ein wesentlicher Bestandteil einer Zustimmung zur Datenverwendung (gemäß Artikel 4 Z 11 DSGVO).

MS gibt **europäische Kundinnen- und Kunden-Daten 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.[8] Man muss MS zugutehalten, dass es einen detaillierten Report im Zuge der Corporate Social Responsibility erstellt.
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."[9]

Es stellt sich die Frage, auf Basis welcher **Rechtsgrundlage** MS 365 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 dann zu prüfen, ob nicht „die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen" – so weit die Rechtslage.

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 seitens MS **intransparent** sei und nach wie vor **Datenübermittlungen in die USA** stattfinden.[10]

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".[11] 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.

Microsoft Deutschland legt am 11. August 2022 noch nach, und bringt das Wohl der Nation aufs Tapet: „Nur konsequente Digitalisierung mit Technik auf dem Stand der Zeit wird es in Deutschland ermöglichen, seinen Wohlstand zu wahren, seine Werte zu verteidigen und seinen gesellschaftlichen Aufgaben erfolgreich nachzukommen (etwa dem Bildungsauftrag)."[12] Sieht man sich diese Argumentationen von MS an, bei der es unter anderem um Werte, Wohlstand und Bildung geht, kann man durchaus zu dem Schluss kommen, die Software von MS habe ziemlich unbegrenzten Einfluss – nämlich auch auf ethischer (Werte), ökonomischer (Wohlstand) und politischer (Bildungsauftrag) Ebene. Ein durchaus naheliegender Schluss, setzt sich MS doch im Zuge der Unterstützung der Ukraine im Krieg gegen Russland dafür ein, die Cyberangriffe von russischer Seite aufzuklären.[13]

8 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE57AOD (report vom Juni 2022, letzter Zugriff: 14.3.2023)
9 https://news.microsoft.com/de-de/im-daten-dschungel-wie-microsoft-mit-dem-cloud-act-umgeht/ (Letzter Zugriff: 14.3.2023)
10 https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS 365_zusammenfassung.pdf (Letzter Zugriff: 14.3.2023)
11 https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/2022.11_Stellungnahme-MS-zu-DSK_25NOV2022_FINAL.pdf (Letzter Zugriff: 14.3.2023)
12 https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/08/Microsoft-Statement_Datenschutzkonformitaet-von-Microsoft-365-und-Microsoft-Teams.pdf (Letzter Zugriff: 14.3.2023)
13 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (Letzter Zugriff: 14.3.2023)

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 im Hintergrund verarbeitet werden.
- Ein eindeutiger Zweck für die zahlreich angebotenen Apps ist nicht immer gegeben.
- Es ist nicht eindeutig feststellbar, wann MS Daten im Auftrag seiner Kundinnen und Kunden verarbeitet und wann es die Daten der Nutzer:innen für eigene Zwecke verarbeitet.
- MS löscht personenbezogene Daten nach Erbringung der vereinbarten Leistung nicht immer. Insbesondere Daten zur „Cyberabwehr" werden nicht vernichtet (bzw. zurückgegeben).
- Datenschutzfolgenabschätzungen werden unzureichend durchgeführt.

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 effektiv abzuschalten (Pseudonymisierung oder „Opt-Out").

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). Diese Vorgaben gelten selbstverständlich ebenso, wenn MS 365 im Betrieb eingesetzt wird. Zwar beziehen sich diese Vorgaben nicht explizit auf Software von MS, jedoch sind die allgemeinen Bestimmungen auch bei MS 365 zu berücksichtigen.

Gefahrenverhütung

Die vielfältigen Kommunikationskanäle, die vielfältigen – mitunter versteckten – Überwachungsmöglichkeiten und die vielfältigen Verknüpfungen bei MS 365 sind durchaus geeignet, die psychische und physische Gesundheit zu beeinträchtigen und bieten somit 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 dann auch in einer BV festgehalten werden (z. B. Deaktivieren der Statusinformation, Begrenzen der Kommunikationskanäle, Recht auf Abschalten etc.).

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 Auflistung vor, wobei die nächste Stufe erst betreten wird, wenn die vorangehende erfolglos blieb (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"**.

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.

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 freigeschaltet oder E-Mailregelungen eingerichtet werden.

Ⓞ**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.

Ⓟ**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 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).

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

Evaluierung

Dass evaluiert werden muss, kann sowohl aus dem ASchG abgeleitet werden als auch aus der DSGVO. Diese sieht vor, dass eine sogenannte Datenschutzfolgenabschätzung (S. 17) 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 ausgestaltet 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.

Die Evaluierung sollte sich folgenden Fragen widmen:

- Was hat sich seit der letzten Evaluierung geändert?
- Sind die Auswirkungen auf die Privatsphäre der Beschäftigten, auf ihre Menschenwürde zu einschneidend? Ist die Überwachung übertrieben – oder ist sie tatsächlich unumgänglich? Kommt es zu einer zu starken Steuerung der Beschäftigten oder bleibt genügend eigener Entscheidungsspielraum?
- Ist es zu Problemen gekommen? Können (neue) Einstellungen abgeändert werden? Sollten bestimmte Erweiterungen/Funktionen abgeschaltet werden?
- Muss – weil die voranstehenden Fragen überwiegend mit „ja" beantwortet wurden – die BV adaptiert werden?

Verschiedene Fragestellungen sollten im Zuge einer Evaluierung beantwortet werden. Wer führt sie durch? Wer wird beteiligt? Mit welchen Methoden wird evaluiert? Braucht es einen Fragebogen/ Interviews/ Beobachtungen/ Hilfe vom Arbeitsinspektorat...? Wo liegt der Fokus? In welchen Abständen wird evaluiert? Die genaueren Abläufe einer Evaluierung sollten jedenfalls in einer Betriebsvereinbarung festgehalten werden.

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).

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, die Person abgestimmt sein und könnten darin bestehen, dass an Beschäftigten sicherere Geräte ausgehändigt werden („Substituierende Maßnahme"), dass bestimmte Features deaktiviert werden („Technische Maßnahme"), dass vermehrt Unterweisungen in der Handhabung von Privacy-Einstellungen von MS 365 stattfinden („Organisatorische Maßnahme") oder dass einzelne Beschäftigte zu bestimmten Apps keinen Zugang mehr erhalten („Personelle Maßnahme").

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. 42], Sharepoint [S. 60], Yammer [S. 57]), es werden andere Mittel für die Erstellung von Dienstplänen verwendet (z. B. Planner [S. 53], Project [S. 75], Forms [S. 54]), es werden Weiterbildungen und Seminare mit digitalen Mitteln online abgehalten (z. B. Teams [S. 42], Sway [S. 59]) 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. 33] 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 [siehe S. 22] und die BV bei Bedarf angepasst wird.

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

DIE ENTSCHEIDUNG DES BETRIEBSRATES

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 generell 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 (etwa, indem die Einsicht von Vorgesetzten in bestimmte Datenanalysen unterbunden wird). In der BV können durch klare Regeln überschießende Leistungskontrollen der Beschäftigten unterbunden werden, es kann das Durchleuchten der Beschäftigten hintangehalten werden.

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 App 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 Angebot an Apps. Es ist also betriebsabhängig, auf welche Art (wie), zu welchem Zweck (wozu), in welchem Ausmaß (wieviel) MS 365 jeweils verwendet wird.

Es bestehen vielfältigste Kombinations- und Erweiterungsmöglichkeiten. Ein Muster für eine Betriebsvereinbarung könnte diesen unzähligen Möglichkeiten nicht gerecht werden – die Gewerkschaft GPA bietet daher auch kein solches Muster an.

Im Drei-Schritt zur Betriebsvereinbarung

Schritt eins: Verschaffe dir einen Überblick über Anwendungen im Betrieb. Die Checkliste der MS 365 Apps [S. 73] hilft dabei.

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

Schritt zwei: Stelle fest zu welchem Zweck eine App verwendet werden soll.

WOZU sollen die MS 365 Apps 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. 71] 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.

ALLGEMEINE GESTALTUNG

WIE SOLL MS 365 GEREGELT WERDEN?

Es hilft beim Arbeiten mit MS 365 einige grundlegende Prinzipien zu beachten, unabhängig davon, welche Lizenzen, Apps, erweiterten Services etc. genutzt werden. Ein Überblick zu den möglichen Anwendungen findet sich in den beiden Checklisten im Anhang „was in einer (Basis-)Betriebsvereinbarung zu regeln ist“ [S. 71] und Checkliste der MS 365 Apps [S.73].
Dieser Teil der Broschüre stellt dar, worauf das Augenmerk gelegt werden sollte, wenn eine grundlegende Betriebsvereinbarung zu MS 365 ausverhandelt wird.

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“.

Folgende Punkte gilt es generell beim Abschluss einer Betriebsvereinbarung zu bedenken:

Die **Zweckbindung** muss eindeutig sein. Es muss klar ersichtlich sein, welche Daten wofür verwendet werden. Die Zweckbindung kann allgemein formuliert werden (siehe Beispiel im grauen Kästchen) aber auf jeden Fall soll sie für eine spezielle Anwendung klar dargestellt werden (z. B. Speichern von Sprachnachrichten bei Gesprächen mit Kundinnen und Kunden mit dem Zweck, gesetzliche Haftungsansprüche klären zu können).

> *aus einer Präambel: Die Betriebsvereinbarung dient dazu, die Interessen der Arbeitnehmer:innen zu wahren, ihre Persönlichkeitsrechte, ihre Privatsphäre und ihre Gesundheit zu schützen. Die Software wird eingesetzt, um eine stabile und sichere Verwaltung der Kommunikation zu gewähren und eine mobile Kommunikation zu gewährleisten.*

> *Die in MS 365 erzeugten Verhaltensdaten dürfen für operative Zwecke in konkreten Einzelprojekten sowie durch Systemadministratoren und -administratorinnen für technische Zwecke genutzt werden, nicht jedoch zur gezielten personenbezogenen oder personenbeziehbaren systematischen Auswertung.*

Aus der Zweckbindung ergibt sich, wer welche **Berechtigung** erhalten muss. Ist der Zweck beispielsweise das

Vermeiden von Virenbefall, sind IT-Administratoren und -Administratorinnen diejenigen, die eine Berechtigung brauchen. Nur so ist gewährleistet, dass der Zugang zu bestimmten Inhalten auch nur denjenigen zur Verfügung steht, die sie für ihre Arbeit 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.

Die Rollenbezeichnung „globaler Leser" ermöglicht es, sämtliche Aktivitätsprotokolle von MS 365 zu sehen. Nicht möglich ist damit das Verfassen, Abändern oder die Einsicht in (persönliche) Inhalte. Die Rolle wird zwar in den Betrieben nur selten an die Arbeitnehmer:innen-Interessenvertretung vergeben, würde sich aber gut für die Betriebsratsarbeit eignen, da sie einen umfassenden Überblick verschaffen würde. Als Alternative kann der Betriebsrat oder die Betriebsrätin auch eine andere Rolle mit umfassenden Leserechten für sich sicherstellen (z. B. Message Center Reader, Reports Reader, lesender Zugriff auf das Azure Active Directory oder Ähnliche). Jedenfalls braucht es eigenständige Einsichtsrechte.

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 erhält sechsmonatlich ein aktualisiertes Berechtigungskonzept. Zur einseitigen Abänderung des Berechtigungskonzepts ist die oder der Arbeitgeber:in nur hinsichtlich der Übertragung von Aufgaben, die ausgeschiedene Mitarbeiter:innen ausgeübt haben, befugt. Alle weiteren Änderungen bedürfen des Einvernehmens der Betriebsparteien.

Manche Funktionen in MS 365 bauen auf langfristig auswertbaren personenbezogenen Datenhistorien auf (Delve [S. 47]). Die gesetzliche Vorgabe 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.

Auswertungsmöglichkeiten müssen auf ein vernünftiges Maß reduziert werden. Zum gemeinsamen Bearbeiten von Dokumenten oder zum Nachverfolgen der einzelnen Änderungsschritte kann eine Anzeige von Verhalten einzelner Nutzer:innen durchaus sinnvoll sein (z. B. wer hat welchen Kommentar eingefügt). Eine personenvergleichende Analyse ist hingegen hintanzuhalten (z. B. wer am häufigsten Änderungen in Dokumenten vornimmt). Die verwendeten Daten sind dabei dieselben, egal ob die Analyse der Daten zweckmäßig ist oder überschießend oder gar gesetzeswidrig. MS 365 erzeugt sie automatisch, mitsamt Datum und Zeitangabe, weshalb in einer BV je nach Verwendungszweck differenziert werden muss.

Die Einstellung im Benutzerkonto „optional verbundene Erfahrungen" in der Rubrik „Datenschutz" zu deaktivieren, ist empfehlenswert, möchte man unerwünschte Datensammlungen einschränken.

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 nicht selten vor offiziellem Arbeitsbeginn gelesen, Dokumente nach Arbeitsende bearbeitet. MS 365 bietet mehrere Apps an, die zur Kommunikation genutzt werden können (z. B. Outlook [S. 39], Teams [S. 42], Sharepoint [S. 60], Yammer [S. 57] 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.

Microsoft 365 erzeugt Daten, die es ermöglichen, die Leistung und das Verhalten von Beschäftigten nachzuvollziehen, zu bemessen oder zu vergleichen (z. B. Versionsverläufe). Diese Daten dürfen aber nicht für den Zweck genutzt werden, das Verhalten oder die Leistung einzelner Arbeitnehmer:innen zu analysieren oder einander gegenüberzustellen, zu prüfen, zu messen, zu beurteilen oder in anderer Weise zu kontrollieren. Ausnahmen sind zulässig, wenn sie zur Erfüllung einer gesetzlichen Pflicht erforderlich sind (wobei die gesetzliche Grundlage dem Betriebsrat bekannt gegeben werden muss), wenn sie in einer Betriebsvereinbarung vereinbart wurden (wobei die betreffende Betriebsvereinbarung im Betrieb allen Beschäftigten bekannt gegeben werden muss) oder wenn der Betriebsrat im Einzelfall zugestimmt hat (wobei diese Zustimmung schriftlich zu dokumentieren ist). Die Auswertung anonymisierter Daten unterliegt keiner Beschränkung, solange die Gruppen zumindest zu zehn Personen zusammengefasst werden.

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, Serien, 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 Cloud).

Eine große Menge von Tools 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 unglaublich erweitert, ohne dass der oder die Nutzer:in den Eindruck hätte, die Welt von MS 365 verlassen zu haben. 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.

Damit die Unzulänglichkeiten 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 man auf die Analyse von Leistungs- oder Verhaltensprofilen oder gar Prognosen seitens Vorgesetzter oder der IT-Abteilung verzichtet. Insbesondere grafische Anzeigen des Arbeits- bzw. Erledigungsstands der Kollegen und Kolleginnen dürfen nicht dazu herangezogen werden, Leistung und Verhalten zu kontrollieren oder bestimmte Beschäftigte(-ngruppen) zu diskriminieren. Ein Generalverbot der Leistungs- und Verhaltenskontrolle – 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.

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.

Sollten Auswertungen das (angebliche) Fehlverhalten von Beschäftigten beinhalten, so ist ein Vorgehen zu vereinbaren, damit diese Auswertungen nur zu konkreten Anlässen stattfinden, der Sachverhalt, also das (vermutete) Fehlverhalten, geklärt sowie „Beifang" vermieden und überschießende Folgen von personenbezogenen Auswertungen 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 ein weiterer Formulierungsvorschlag:[14]

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 und weitere als anderwärtig vereinbarte personenbezogene Datenauswertrungen vornehmen. Dem Betriebsrat wird ein vollständiges Protokoll der eingesehenen Nutzerdaten zur Verfügung gestellt.

Zu jeder in Betrieb befindlichen Anwendung ist unbedingt eine **Schulung** anzubieten. Vor allem in der ersten Einführungsphase sind Trainer:innen/Lernbegleiter:innen/Experten und Expertinnen für die Beschäftigten von großem Nutzen und sollten daher in der BV angegeben werden. In einigen Betrieben werden sogenannte „Champions" ernannt, die als Ansprechpersonen zur Verfügung stehen [siehe S. 33]. 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 „optionale 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

14 „7 Tipps für eine BV Microsoft 365" in: Computer und Arbeit 9/2022, Bund Verlag. (Anmerkung: die Verwendung von ganzen Muster-BVen ist kritisch zu sehen, da MS 365 doch sehr Unterschiedliches beinhaltet.)

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 „Champion", die die Gruppen in Microsoft 365 Anwendungen administrieren.

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.

Es gibt die Möglichkeit, Updates und deren neue Features vorab zu testen. Das kann für den Kunden oder die Kundin so eingerichtet werden, indem der sogenannte „Tenant" (engl. „Mieter") des Cloudservices diese Berechtigung zum Freischalten von Updates erhält. Der Betriebsrat kann sich in diese Testphase hineinreklamieren und so die bevorstehenden Änderungen, von MS auch „neue Erfahrungen" genannt, auf ihre Auswirkungen und Sinnhaftigkeit hin überprüfen.

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.

MS 365 wird sukzessive unter Beteiligung des Betriebsrats in Betrieb genommen, einzelne Module zunächst testweise und auch nur bei einem begrenzten Personenkreis eingesetzt.

Dass der Betriebsrat eingebunden wird, sollte auch in einer 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 [sowie des regulären Betriebs], (...) Zugang zu allen relevanten Unterlagen und Dokumentationen.[15]

15 „Betriebsrat als Testuser" in: Computer und Arbeit 1/ 2023, Bund Verlag

Zu den Updates können folgende Vereinbarungen getroffen werden:
Die BV kann 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, wobei folgende Leitfragen gelten:

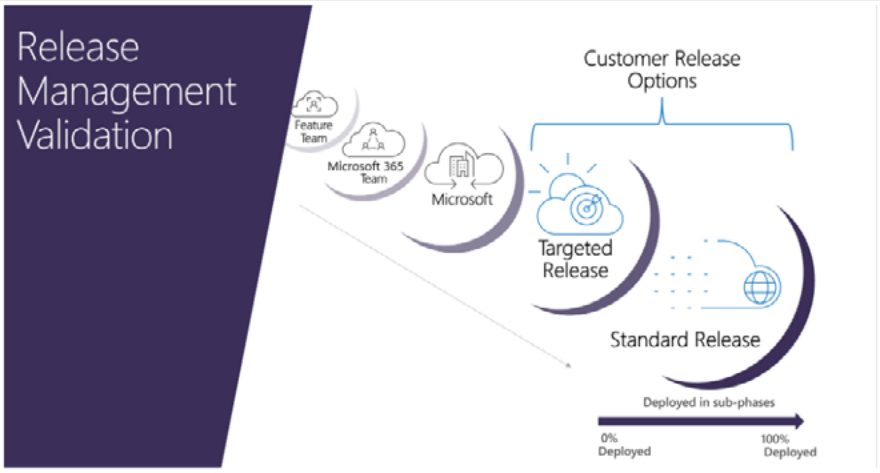
- Tangiert das Update die Speicherung von Beschäftigtendaten?
- Tangiert das Update die Auswertung von Beschäftigtendaten bzgl. Leistungs- und Verhaltenskontrolle?
- Ändert sich durch die Updates die Arbeitsorganisation/Zusammenarbeit (z. B. durch permanente Anzeige des Präsenzstatus, automatische Übernahme von Terminanfragen aus Teams)?
- Hat das Update Auswirkungen auf die Qualifizierung der Beschäftigten (z. B. Trainingserfordernisse)?
- Sind die Einstellungen im Admin-Center (insbesondere die Deaktivierung von Delve [S. 49]) nach dem letzten Update noch so, wie sie es zuvor waren?

Aktualisierungen/Updates werden regelmäßig von Microsoft 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 Releases stellt MS 365 auf einer eigenen Webseite übersichtlich dar: https://m365maps.com/changes.htm

Es ist ratsam, hier regelmäßig nachzusehen, um sich auf dem Laufenden zu halten.

VORGEHEN BEI DER INSTALLATION VON NEUEN MS 365-VERSIONEN



Bei wichtigen Updates werden Kunden zunächst von der Microsoft 365-Roadmap benachrichtigt. Wenn ein Update dem Rollout näher kommt, wird es über Ihr Microsoft 365-Nachrichtencenter kommuniziert.

ⓘ Hinweis

Sie benötigen ein Microsoft 365- oder Azure AD-Konto, um über das **Admin Center** auf Ihr Nachrichtencenter zuzugreifen. Benutzer des Microsoft 365 Home-Plans verfügen nicht über ein Admin Center.

Manche Betriebe ernennen auf Anraten von Microsoft bei der Einführung von MS 365 **„Champions“**. In anderen Betrieben nennt man die „Champions“ „PowerUser:innen“ oder „KeyUser:innen“. Sie sind in der Regel aus dem Kreis der „normalen“ Nutzer:innen und werden eigens zu den unterschiedlichen Anwendungen von MS 365 geschult bzw. von der alltäglichen Arbeit teilweise freigestellt, um die Apps besser kennenzulernen, sie besser zu durchschauen, mit den Apps von MS 365 zu „spielen“ – wie es ein Champion ausdrückt. Sie bringen idealerweise Interesse an technischen Abläufen und Neugierde mit. Geduld und didaktisches Geschick ist ebenso von Vorteil, denn Champions sollen ihre Kenntnisse an die Belegschaft weitergeben. Wenn also Unklarheiten auftauchen, soll der oder die Beschäftigte sich nicht sofort an den üblichen 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.

MS 365 ist ein sehr flexibles und schnelllebiges Programm, das daher auch einer anpassungsfähigen Auskunftsstelle bedarf. Idealerweise stehen auch nach der Ausrollung und 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 spontan und bedarfsorientiert anwesende Stelle könnte auch in die BV aufgenommen werden.

Eine eigene, mit möglichst fixen Mitgliedern zusammengesetzte **„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 oder externer Sachverständiger), 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 (siehe dazu auch „interne Personaldatenschutzkommission" in der Rahmen-Datenschutz-BV der Gewerkschaft GPA).

Auf vielen MS Anwendungen können die Nutzer:innen eigene Profile anlegen (z. B. MS-Teams [S. 42], Sharepoint [S. 60]). 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.

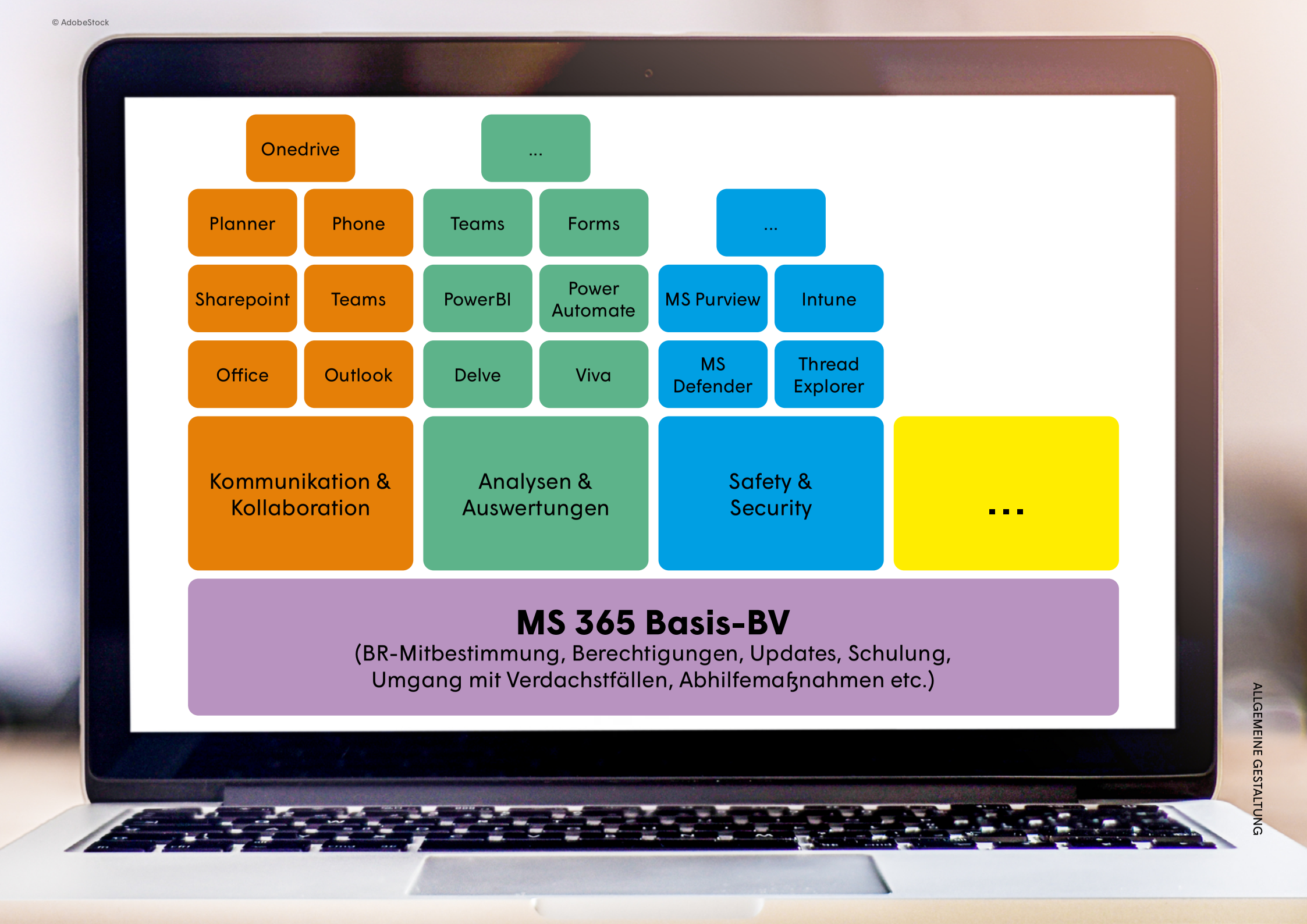
Um Zusatz-Betriebsvereinbarungen zu einzelnen Apps oder deren Funktionen abzuschließen, muss ein Überblick bestehen, welche Teile von MS 365 konkret verwendet werden (siehe Checkliste „Zu den Apps, die im Betrieb im Einsatz sind" [S. 73–76]). Ist unklar, welche genau im Einsatz sind, dann laufen BV-Verhandlungen gegenstandslos im Kreis. Zu den Apps, die im Betrieb im Einsatz sind, kann aufbauend auf einer Basis-BV gezielt die jeweils passende Musterbetriebsvereinbarung der Gewerkschaft GPA als Inspirationsquelle für konkrete Formulierungen herangezogen werden. Die Gewerkschaft GPA bietet zahlreiche Muster-BVs zu einzelnen Systemen an, wie bspw. zu E-Mail/Internet (MS Outlook S. 39), Telefon (MS Teams Phone), Videokonferenzsysteme (MS Teams), Mobile Device Management (Intune S. 69) etc. Für die einzelnen Anwendungen sollte dann jeweils 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 NutzerInnen der österreichischen Standorte zu deaktivieren.

Zusammenfassung der wichtigsten Regelungspunkte in einer Basis-Betriebsvereinbarung zu MS 365:
(siehe auch Checkliste im Anhang S. 71)

- Enge Zweckbindung definieren
- Berechtigungskonzept (= Zugriffskonzept, Rollenkonzept) erstellen
- Auswertungs- und Überwachungsmöglichkeiten beschränken
- Löschkonzept erstellen
- Privatnutzung festlegen
- Freiwilligkeit festlegen wo möglich
- Schulungsplan erstellen
- Vorgehensweise bei Fehlverhalten vereinbaren (= „stufenweise Kontrollverdichtung")
- Vorgehensweise bei Updates (= Aktualisierungen, Releases, Verbesserungen) vereinbaren
- Ansprechpersonen definieren
- MS 365 Experten- und Expertinnen-Gruppe installieren
- Regelmäßige Evaluierung (sowohl der Risiken für die Privatsphäre sowie der Gesundheitsrisiken) durchführen

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**, die verschiedenen Apps nach Funktionen zusammenzufassen (z. B. Kommunikation, Sicherheit, Zusammenarbeit 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 und daher doppelt geregelt werden müssen. Gleichzeitig kann der Nachteil entstehen, dass die Verhandlungen ausufern, weil der sachliche Geltungsbereich erst geklärt werden muss. Welche Strategie gewählt wird, ist Entscheidung des Betriebsratsgremiums.



DIE EINZELNEN APPS

EINE AUSWAHL

In dem Teil der Broschüre werden jene Anwendungen von MS 365 skizziert, die in den Beratungen der Gewerkschaft GPA häufig auftreten, also weithin bekannt sind und in zahlreichen Betrieben zum Einsatz kommen wie beispielsweise extrem rasch weiterentwickelte und ausgebaute App Teams [S. 42]. Außerdem sind diejenigen Apps dargestellt, die Besonderheiten aufweisen, wie beispielsweise ein besonders hohes Überwachungspotential bei MS Dynamics [S. 53] oder die äußerst fragliche Sinnhaftigkeit von Viva [S. 50]. Das Paket MS 365 umfasst wesentlich mehr Programme als in dieser Broschüre angeführt sind, wie die Checkliste zu den Apps im Anhang [S. 73] oder ein Blick auf den letzten MS-365-Release im Januar 2023[16] zeigen.

MS 365 möchte gerne ein Produkt für alle Anforderungen anbieten. Man kann die verschiedenen Anwendungen grob in drei Sparten für drei Zielgruppen unterteilen. Jede Sparte hat eine Anwendung in der die Dokumente, Arbeitsaufgaben, Termine, Prozesse strukturiert verwaltet und gesteuert werden.

1. Die einzelnen Nutzer:innen verwenden als persönliches Ablagesystem hauptsächlich OneDrive.

2. Die verschiedenen Einheiten eines Unternehmens (also beispielsweise Abteilungen, Gruppen, Teams, Standorte) arbeiten auf Teams zusammen.

3. Die Leitung eines Unternehmens managt den Gesamtbetrieb auf Sharepoint.

Im Hintergrund sind freilich die Anwendungen miteinander verbunden, synchronisiert. Was also einzelne in ihren persönlichen Bereich stellen kann, wenn es freigegeben wurde, auch in Teams eingesehen und über Sharepoint verwaltet werden.

Manche Aufgaben können mit Hilfe mehrerer Apps erledigt werden. So kann beispielsweise sowohl der Planner als auch ToDo oder ein Channel in Teams für das Projektmanagement verwendet werden, um Aufgaben zu verteilen oder einen Zeitablauf festzulegen.

Auch ein Ablagesystem oder ein Dokumentenmanagement ist in mehreren MS 365 Apps möglich. Geeignet sind sowohl OneDrive als auch Teams und dessen einzelne Channels als auch Sharepoint. 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, dürfen, müssen, ist auch 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 Aufgabenverteilung, die befolgt werden muss? Ein wesentlicher

16 https://m365maps.com/files/Microsoft-365-Business-All.htm

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 Apps/Anwendungen/Module unterteilt in solche für „normale" **Nutzer:innen**/Kollegen und Kolleginnen/Beschäftigte und solche, die eher für **Administrator:innen** gedacht sind. Die Grenzen sind hier fließend, da mitunter Apps für System-Administratoren auch gewöhnlichen Nutzer:innen zur Verfügung stehen können.

Die folgenden Kapitel enthalten graue Kästchen. Jene mit einem Anführungszeichen beinhalten Beispiele aus bestehenden (Muster-)Betriebsvereinbarungen. Jene mit Pfeilchen enthalten praktische Tipps. Jene mit Diamanten Besonderheiten. Am Ende jedes Kapitels sind die wichtigsten Punkte, denen man sich in einer Betriebsvereinbarung zur jeweiligen App, widmen sollte, aufgezählt.

Legt im Betrieb fest, welche Apps wofür verwendet werden sollen. Das vermeidet Redundanzen und Unklarheiten.

USER-APPS

Damit sind Anwendungen von MS 365 gemeint, die für jeden Nutzer und jede Nutzerin üblicher Weise zur Verfügung stehen.

OFFICE (= WORD, EXCEL, POWERPOINT)

Bei Office handelt es sich um die wohl bekannteste Anwendung von MS. Sie dient dem Verfassen von Dokumenten (Word), dem Erstellen und Berechnen von Tabellen (Excel) oder 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, um beurteilen zu können, was dahintersteckt und ob und wo Gefahren lauern.

Word erfasst personenbezogene Daten, die Auskunft über das Verhalten der Nutzer:innen geben. Wer hat das Dokument erstellt? Wer hat wann welche Änderungen vorgenommen? Um welche Uhrzeit wurde ein Dokument oder eine Tabelle mit welchem Ergebnis bearbeitet? Diese und andere Informationen werden gespeichert und können zur Verhaltensanalyse herangezogen werden. Die Speicherung erfolgt automatisch und kann nicht abgedreht werden. Die „Lebensgeschichte" jedes Dokuments ist mit mindestens einhundert bis zu maximal fünftausend Versionen vorhanden. Darüber hinaus werden die Dokumente, so sie auf Sharepoint [S. 60] oder OneDrive [S. 55] abgelegt werden, in sämtlichen Versionen gespeichert. Zwar lässt sich die Anzahl der gespeicherten Versionen konfigurieren, einhundert ist jedoch (Mit Stand Ende 2022) das Minimum an Speicherungen. Darüber hinaus schreibt Graph [S. 49] im Hintergrund immer mit und verknüpft die Daten mit denen aus anderen Anwendungen.

Seit 2022 bietet Office eine Liste **empfohlener Dateien** auf der Registerkarte „Datei" auf der Startseite von Word, Excel oder PowerPoint an. Damit soll den Nutzer:innen geholfen werden, die Arbeit – auch anderer Kolleginnen – „nachzuverfolgen und schnell auf Dateien mit Aktivitäten zuzugreifen, die Sie am meisten schätzen, z. B. Bearbeitungen, Erwähnungen, Kommentare von Personen, mit denen Sie interagieren."[17]

MS schreibt weiter: „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.

> *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.*

Es besteht Regelungsbedarf:

- Speicherort festlegen (z. B. wo werden gemeinsam zu bearbeitende Dokumente abgelegt? Wo werden besonders schützenswerte Daten (nicht) abgelegt?)

17 https://support.microsoft.com/de-de/office/empfohlene-dateien-in-office-232c8322-1060-4453-bd69-a4770efe731e

- Berechtigungskonzept festlegen (wer hat worauf Zugriff?)
- Umgang mit der „empfohlene Dateien"-Liste festlegen (muss sie eingeschalten sein? Muss sie verwendet werden? Müssen die Dokumente/Tabellen/Präsentationen gelesen/bearbeitet werden?)
- Speicherdauer festlegen (wie lange müssen welche Dokumente aufbewahrt werden? Soweit technische Möglichkeiten dazu vorhanden sind, ansonsten organisatorische Regelungen festlegen)
- Interpretationen zu Arbeitsleistung und Verhalten unterbinden, arbeitsrechtliche Maßnahmen ausschließen
- Klassifikation der Dokumente nach ihrer Geheimhaltungsstufe (damit einhergehend Zugriffsrechte und Speicherdauer)

Die Funktion „Datei folgen" sollte nur dann benutzt werden, wenn sie tatsächlich benötigt wird.

Die Funktion „Mich bei Änderungen von Elementen benachrichtigen" kann in der Regel getrost abgeschaltet werden, da die Nutzer:innen meist nicht über jeden geänderten Beistrich ein E-Mail ins Postfach bekommen wollen.

OUTLOOK (= E-MAIL, KALENDER, KONTAKTE)

Outlook verwaltet Termine, Notizen, Aufgaben, Adress- und Telefonbuch, E-Mails und Postfächer. 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 werden im Hintergrund über Graph [S. 49] umfassend Daten gespeichert. Administratior:innen sehen, wer wann welche Betreffzeile an wen versendet hat. Diese Standardanzeigen sind immer in Exchange [S. 64] verfügbar und können technisch nicht abgeschaltet werden. Im Exchange-Server [s S. 64] können Regeln erstellt werden, wie mit E-Mails und anderen Outlook-Komponenten umgegangen werden soll.

Im **E-Mail-**Programm von Outlook gibt es die Einstellung „Posteingang mit Relevanz" (vormals „Clutter" genannt). Ist sie aktiviert, werden „selbstlernend" Prioritäten für E-Mails erstellt. MS ordnet, was für die Nutzer:innen wichtig ist und was nicht. Anhand der von den Nutzer:innen selbst markierten, also bewerteten E-Mails (z. B. wichtig/ zur Nachverfolgung/erledigt) sowie hinterlegter Hierarchien „lernt" Outlook, welche Absender:innen schnelle Antworten erfordern (z. B. die der Vorgesetzten), welche erst später Rückmeldung erfordern oder welche Inhalte aufgrund der Betreffzeile gar keinen Aufschub erlauben. Dem Arbeiten mit

E-Mails wohnt also automatisch eine gewisse Verhaltenskontrolle inne.

Es empfiehlt sich „Postfach mit Relevanz" nicht zu aktivieren und regelmäßig zu überprüfen, ob die Funktion tatsächlich noch inaktiv ist.

Zu E-Mails sollte in der BV geregelt werden:

- Speicherdauer; welche E-Mails werden automatisch aufbewahrt? Welche E-Mails sind manuell aufzubewahren bzw. zu löschen? betreffen Aufbewahrungsregeln auch manuell von den Nutzer:innen gelöschte E-Mails?

Von den Beschäftigten manuell gelöschte E-Mails werden ein weiteres Quartal im Papierkorb aufbewahrt und werden mit Ende des darauffolgenden Quartals unwiederbringlich gelöscht.

Vertretungsregelungen festlegen; Wer darf in das Postfach Einsicht nehmen, wenn jemand plötzlich abwesend ist? Welchen Text sollte die Abwesenheitsnotiz bei geplanten Abwesenheiten enthalten? Wer vertritt eine abwesende Kollegin oder einen abwesenden Kollegen, wenn E-Mails zu beantworten sind?)

- Benachrichtigungen aus Teams [s S. 42], Viva Insigth [s S. 50] und ähnlichen Tools deaktivieren, um überbordende Kommunikation zu vermeiden

- Benachrichtigungen über Statusänderungen [s S. 52] für andere Nutzer:innen deaktivieren

- Vertretungs- und Weiterleitungskonzept sowohl für geplante Abwesenheiten also auch für Notfälle; Vorgesetzte sollten nur in Notfällen die E-Mails der Arbeitnehmerinnen und Arbeitnehmer sehen oder an andere weiterleiten

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)

Generell ist die Privatnutzung im üblichen Rahmen erlaubt. Dafür steht allen Beschäftigten des Unternehmens ein persönlicher Ordner zur Verfügung. Die Arbeitnehmer:innen sind allerdings angehalten, keine Accounts für die Privatnutzung einzurichten (z. B. Konten für Online-Handel) und keine Ordner für regelmäßig stattfindende private Zwecke anzulegen (z. B. für Sportvereins-Newsletter). Die Privatnutzung ist gestattet, solange sie maßvoll ist und die Arbeitsleistung nicht beeinträchtigt.

Es ist erlaubt MS 365 für private Zwecke zu verwenden, solange es die betrieblichen Abläufe nicht stört, maßvoll erfolgt und kein Schaden grob fahrlässig herbeigeführt wird.

Stufenweise Kontrollverdichtung festlegen, für den Fall, dass Administratorinnen oder Administratoren 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.

- Zusätzliche Verschlüsselung von E-Mails ermöglichen
- Die Einsichtszwecke von Administrator:innen begrenzen auf Vermeiden von Schad-Software, Angriffen, Datenverlust.

Der **Kalender** dient dazu, die eigene Arbeit zu organisieren oder Termine gemeinsam abzuklären. Kalender sollten nicht der Arbeitszeiterfassung dienen, sondern der Arbeitsorganisation. Über Exchange [S. 64] kann der Kalender – und dessen Statusanzeigen – für alle (freigeschaltenen) Nutzer:inen einsehbar gemacht werden. 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.

Für die Kalenderfunktion können in einer BV folgende Punkte geregelt sein:

- Zwecke festlegen; wird der Kalender für Aufgabenverteilung und -planung verwendet oder eine anderes MS App (z. B. Teams [S. 42], Planner [S. 53], ToDo [S. 51] ...)
- Einsichtsregeln, wer wessen Kalender sehen oder wer Termine ein- und austragen kann, Leseberechtigungen und Schreibberechtigungen sollten von den einzelnen Benutzer:innen selbstbestimmt vergeben
- Einsicht Externer bei Kalendereinträgen unterbinden
- Festlegen, dass der Kalender nicht der Arbeitszeiterfassung und nicht der Dokumentation (erledigter) Arbeitsaufgaben dient
- Keine automatisierten Terminvorschläge
- Keine automatisierte Prioritätensetzung
- Keine Standortangaben freischalten
- Auswertungsverbot von Profilen oder eine konkrete Ausnahmeregelung bei anlassbezogenen, begründeten Verdachtsmomenten unter Beteiligung des Betriebsrats
- Vorschläge für Ruhezeiten oder „well-being“ deaktivieren

TEAMS

Teams kann wesentlich mehr als Videotelefonie. Teams ist eine Plattform für gemeinsames Bearbeiten und Ablegen von Dateien, das Versenden von Nachrichten, die Verknüpfung mit Terminen oder das Chatten (Plaudern) Kommunizieren. Teams ist umfassend zur Zusammenarbeit geeignet, fällt also unter die Bezeichnung: „Unified Collaboration and Communication" (UCC), zu Deutsch: vereinheitliche Kommunikation und Zusammenarbeit.

Teams ist für die Kommunikation – insbesondere seit dem vermehrten Arbeiten im Home-Office – ein gerne genutztes Instrument. Gute Übertragungsqualität und vielfältige Funktionalitäten für vielfältige Medien wie Bild, Ton, Chats, Dokumente etc. ohne lästigen und zeitraubenden Wechsel von einem Format auf ein anderes sorgen dafür, dass MS Teams weit verbreitet ist.

Bei Teams unterscheiden sich die gratis und die in einer bezahlten Lizenz enthaltenen Features. Bei der Gratis-Version stehen in der Regel Videotelefonie und Chatgruppen für die Nutzer:innen im Vordergrund. Die Upload-Kapazitäten (z. B. für die gemeinsame Dokumentenbearbeitung) sind in der Gratis-Variante mit zwei Gigabyte begrenzt; das Aufzeichnen und Vorausplanen von Videokonferenzen ist bei der Gratis-Version ebenso wenig möglich wie die sogenannte „Bildschirmfreigabe", mittels der während dem Video-Call den anderen Teilnehmer:innen Dokumente oder Präsentationen gezeigt werden können (Stand Dezember 2022).

Wird ein neues Team in MS 365 erstellt, sind im Hintergrund sämtliche Informationen aus dem Active Directory [S. 66] verknüpft. Meist geht mit der Erstellung eines Teams ebenso eine Verknüpfung zum Exchange-Server für ein E-Mail-Postfach und Kalenderansichten [S. 64] sowie eine Verbindung zu SharePoint [S. 60] einher.

PRÄSENZANZEIGEN

Benutzerdefiniert	Durch die App konfiguriert
Verfügbar	Verfügbar
	Verfügbar, nicht im Büro. Hinweis: „Außer Haus" wird automatisch für die Zeiträume eingestellt, in denen der Benutzer "automatische Antworten" festlegt. Wenn der Benutzer die App in diesen Zeiträumen verwendet, kann eine doppelte Anwesenheit angezeigt werden wie z. B. „Außer Haus, verfügbar".
Beschäftigt	Beschäftigt
	In einem Anruf
	In einer Besprechung
	Bei einem Anruf, außer Haus
Nicht stören	
	Präsentieren
	Konzentration. Die Fokussierung erfolgt, wenn die Benutzer die Fokuszeit in MyAnalytics/Insights in ihren Kalendern einplanen.
Weg	Weg
	Abwesend letzter *Gesehener Zeitpunkt*
Bin gleich zurück	
Offline anzeigen	Offline. Wenn Benutzer während einigen Minuten nicht auf ihren Geräten angemeldet sind, erscheinen Sie als Offline.
	Status unbekannt
	Nicht im Büro. „Außer Haus" wird verwendet, wenn „automatische Antwort" gesetzt ist.

Prinzipiell bietet das den Vorteil, dass einmal hochgeladene Dateien auf allen Plattformen (z. B. in der Dokumentenbibliothek) verfügbar sind. Werden gemeinsame Zugriffe auf SharePoint, Teams oder OneDrive-Plattformen verschieden eingerichtet, wird es allerdings unübersichtlich. Nutzer:innen sind dann verwirrt von nicht mehr auffindbaren Dateien, Dateien ohne Zuordnung, auf SharePoint vorhandenen obwohl eigentlich gelöschten Unterlagen etc. Um derartige 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 jedoch erhalten bleibt.

Die Übersetzungsfunktion von **Sprache** in Text wird immer besser und ist vor allem für internationale Treffen hilfreich (z. B. bei einem Europäischen Betriebsrat). Untertitel sind (derzeit) ausschließlich auf Englisch verfügbar. Falls die Übersetzung der Redebeiträge allerdings gespeichert wird, ist unbedingt eine Überarbeitung erforderlich. Die Sprachassistenz steht außerdem zur Verfügung, um Texte vorzulesen oder Befehle auszuführen.

Über Teams können auch „Spielereien" wie Giphies, Memes oder andere kleine Bildchen mit mehr oder weniger lustigen Inhalten versendet werden (man nennt das auch „Gamification"). Mittels **„Praise"** (also Lob) kann man **Bewertungen** an Kolleg:innen verschicken. MS 365 bietet dieses „Lob" in Form von kleinen Bildchen mit Löwen (der Mutige), Segelschiffen (der Innovative), einer Faust (der Schlagkräftige) usw. an. Nachdem bei diesen „Praise"-Bewertungen getrackt wird, wer wem was wann wie oft geschickt hat, wobei MS beteuert, dass es nur den Empfänger:innen selbst zur Verfügung steht, lautet die Empfehlung sie eher nicht zu verwenden. Der Interpretationsspielraum derartiger Bewertungen ist sehr breit. Die Verwendung der Bildchen kommt dem Spieltrieb entgegen, fördert die Interaktion untereinander und schnell vergeht die Zeit ... Ob derartiges verwendet werden soll, ist Geschmackssache.

Grundsätzlich geht man auf der Teams-Plattform davon aus, dass alle gleichberechtigt darin arbeiten und alle alles sehen. Werden Untergruppen („Channels") eingerichtet mit anderen Leseberechtigungen wird es kompliziert und Teams funktioniert nicht mehr so effektiv.

Ganz ohne Hierarchien geht es auf Teams nicht. Vortragende erhalten beispielsweise 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 die Leiter:innen eines Bereichs, einer Gruppe, einer Abteilung, eines Standorts.

Die Tätigkeiten der letzten sieben bis 28 Tage können mit dem (2020 neu zur Verfügung gestellten) **Analysetool** für die gesamte Gruppe von den „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, also 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. Die Anonymität ist in Teams nur bedingt gegeben. Je kleiner die Gruppe auf Teams oder im Channel desto weniger Anonymität ist gegeben. Daher wird es erforderlich sein, über Bewusstseinsarbeit, Schulungen und Betriebsvereinbarungen zu regeln, dass diese Daten nicht zu unlauteren Zwecken eingesehen und verwendet werden und schon gar nicht zu (nachteiligen) Interpretationen für die Beschäftigten führen.

Graphische 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.

Microsoft bietet Teams seit einem Update im Juni 2021 für bis zu eintausend Personen kostenlos an; davor waren es für Veranstaltungen mit maximal 300 Beteiligten verfügbar.

Teams beinhaltet Funktionen, die je nach Bedarf ein- oder abgeschaltet werden können. Ein- und Ausschalten der einzelnen Funktionen sollte so weit als möglich freiwillig erfolgen. **Kamera-, Mikrofon- und Freigabe** von **Dokumenten** sollte 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, müssten diese Personen darüber informiert werden.

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, Entscheidungen von Gremien), sollte allerdings auf einen engen Zweck beschränkt werden (z. B. konkrete Schadensersatzansprüche, Abstimmungsergebnisse festhalten).

Teams bietet ein **„Sofortprotokoll"**. Besprechungsnotizen können hier für alle Teilnehmenden transparent verfasst werden.

MS Teams zeigt den **„Status"**. Damit können die Nutzer:innen einen der von MS vordefinierten Verfügbarkeitsstatus wählen. Teams gibt dann Auskunft darüber, ob die Kolleg:innen gerade „in einer Besprechung" oder „in einem Call" sind, was aufgrund des Terminkalenders [S. 52] oder der aktiven Telefonfunktion festgestellt wird. Der Status wird aber nicht nur in Teams sondern auch in Outlook [S. 39] und Sharepoint [S. 60] angezeigt. Zusätzlich wertet Delve [S. 47] aus, welche Statusangaben die jeweiligen Nutzer:innen machen. Es fragt sich, ob die Angaben im Arbeitsalltag hilfreich sind (siehe Interpretation von Beschäftigten-Daten [S. 10]). Mitunter führen sie zu einem Rechtfertigungsdruck, warum jemand gerade „nicht verfügbar" ist.

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 Kleinigkeit 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.

Videokonferenzen, Chats und deren Aufzeichnungen werden im Interesse der Kund:innen von MS 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.

Seit Februar 2023 ist **ChatGPT**, die **KI** die in aller Munde ist, auch ein Teil von MS Teams für Premium Abonnentinnen und Abonnenten. ChatGPT soll die Meetings auf Teams „intelligenter, personalisierter und geschützter machen", indem beispielsweise Aufgaben empfohlen, Inhalte zusammengefasst, Protokolle erstellt oder englischsprechende Meeting-Teilnehmende übersetzt werden.

Teams ist in den 2020er Jahren *die* Anwendung von MS, für die Erweiterungen und Optimierungen entwickelt werden, bei der geforscht und Werbung betrieben wird. MS dürfte derzeit viel investieren, um Teams ganz an die Spitze der Kommunikations-und-Kollaborations-Software zu bringen.

Die zahlreichen Verknüpfungen und Funktionalitäten von Teams lassen bei den Nutzer:innen ein bisweilen verwirrendes „Erlebnis" zurück. Es sollte daher eindeutig dargelegt werden, wofür Teams verwendet wird – und wozu es andere Kommunikationskanäle gibt.

Es sollte in einer Abteilung eine gemeinsame Regelung erarbeitet werden, für welche Zwecke Teams genutzt werden soll (z. B. meetings) – und wozu nicht (z. B. das jährliche Mitarbeiter:innengespräch). Bisweilen holen sich für dieses Ziel Unternehmen spezialisierte externe Berater:innen an Bord, deren es mittlerweile eine wachsende Zahl gibt. Jedenfalls sollte sich in einer BV widerspiegeln, dass es unterschiedliche Kommunikationsmittel auf MS 365 gibt, die jeweils für bestimmte Zwecke geeignet sind.

Für Videokonferenzen via Teams sind Regelungen in einer BV zu treffen:

- Zweckbestimmung (z. B. interne Informationsveranstaltung)
- 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)
- Mithören/Aufschalten als Standardeinstellung deaktiviert; auch Administrator:innen-Rechte so einschränken, dass diese keine Aufzeichnungen durchführen können oder nur für sehr eingeschränkte Zwecke (z. B. Schulung).
- Bei Teams-Sitzungen nur das Fenster teilen und nicht den ganzen Bildschirm, damit allfällig offene Seiten/Dokumente nicht von den anderen Teilnehmenden mitgelesen werden können
- Den Umgang mit allfälligen Aufzeichnungen regeln (für wen wird das Recording zur Verfügung gestellt? Wo wird es gespeichert? Wann wird es wieder gelöscht?)
- Freiwilligkeit von Ton- und Bildaufnahmen sowie enge Zweckbindung (z. B. Schulungen)
- empfohlene Standardeinstellung falls im Privatbereich oder mit anderen Personen im Zimmer eine Konferenz stattfindet: Hintergrund verschwimmend
- Verwendung eines Headsets/ Kopfhörer vereinbaren, wenn weitere Personen im Raum sind
- Sind die Konferenzen länger als eine Stunde, sind Pausenregelungen zu treffen (Bildschirmpause)

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

- Ausführliche Schulung als Vorbedingung zur Teams-Nutzung – insbesondere für Teams-Owner, inklusive Privacy-Einstellungen
- Zweck beschreiben (z. B. gemeinsame Dateienbearbeitung im Projekt XY, sind die Dateien auch auf OneDrive und SharePoint mit weiteren Personen geteilt?)
- Berechtigungen festlegen, wer welche Aufgaben in Teams hat. Welche Teams-Mitglieder dürfen was hinzufügen/verändern/sehen? Festlegen, wer die Leitungsfunktion inne hat und wer die Teammitglieder sind
- Download bzw. Auswertung des Teilnahme-Protokolls unterbinden (Technisch oder organisatorisch)
- Ansprechperson bei technischen Problemen
- Festlegen, dass aufgrund der Einsicht in Bearbeitungsprotokolle/Teilnehmer:innen-Listen u.s.w. keine Leistungsbeurteilung und kein -vergleich erfolgen darf
- Festlegen, wann nicht mehr genutzte Teams (samt allfällig angelegten Dateien/ Bibliotheken/ Kanälen/ Arbeitsräumen/ Protokollen/ Videos etc.) nach Projektende wieder gelöscht werden.
- Im Admin-Center die Funktion „alle Apps zulassen" nicht freigeben (Gefahr der Unübersichtlichkeit) ODER: genau regeln, wer weitere Apps mit Teams verbinden darf (IT oder Owner)?

- Festlegen, wofür Chats verwendet werden und falls sie nur zum Plaudern eingesetzt sind, festlegen, dass sie automatisch gelöscht werden

- „Praise"-Verschicken deaktivieren oder jegliche Auswertungen dazu über das Admin-Center unterbinden

- „giphy-Inhaltsbewertung" deaktivieren

- „Memes in Unterhaltungen verwenden" deaktivieren

- Deaktivieren der „Benachrichtigung bei Aktivität" bzw. „dringende Nachrichten mit Priorität senden" deaktivieren; Aktivitätsfeed so einstellen, dass nur ungelesene Feeds eine Benachrichtigung auslösen

- Bei der gemeinsamen Dokumentenbearbeitung sollte keinesfalls der Befehl „Steuerung anfordern" 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 auch zu löschen.

- Freiwilligkeit von Statusanzeigen; keine Auswertung der vorhandenen Statusanzeigen

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

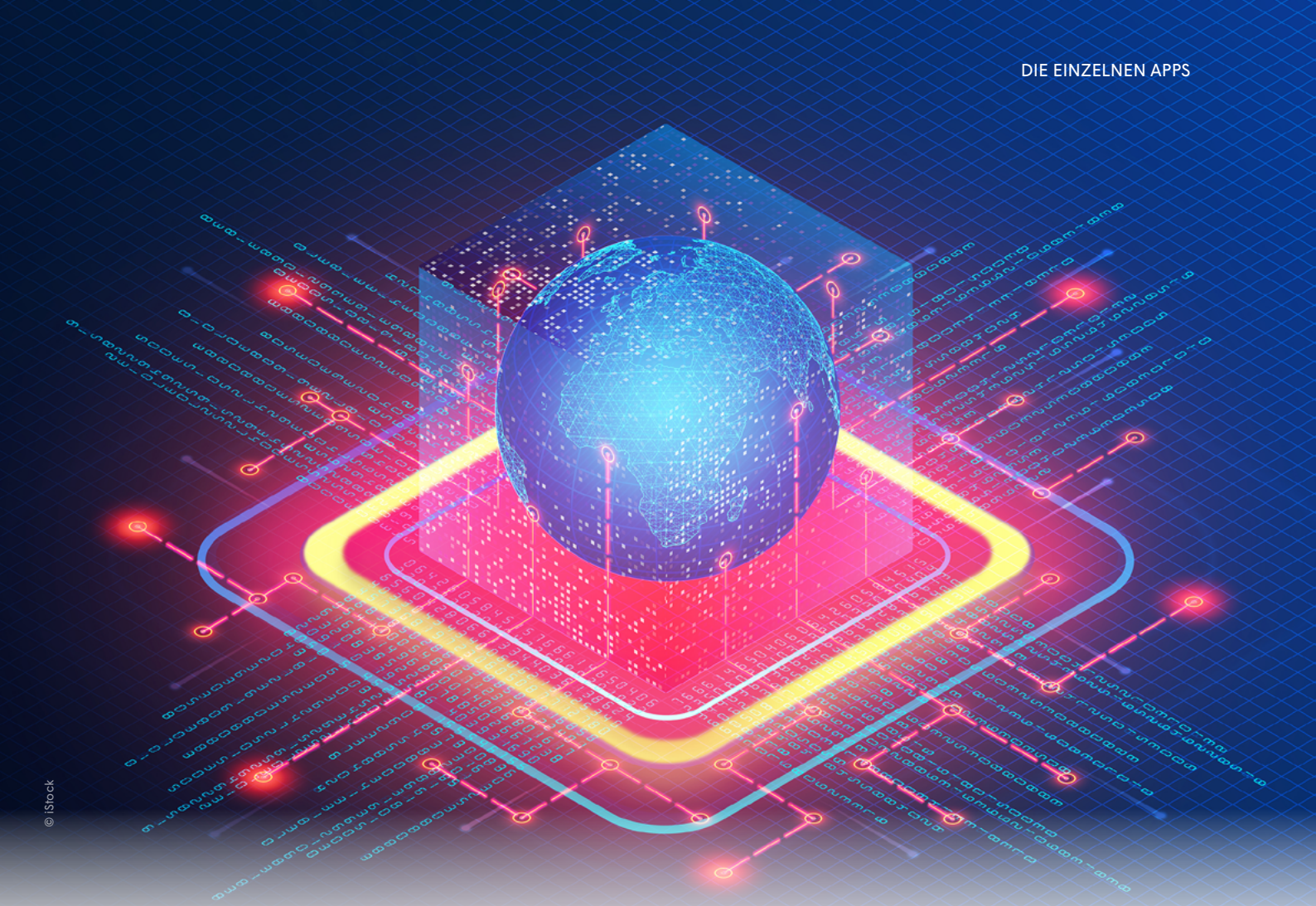
- Umgang mit un-/gelesenen Nachrichten (Anzeige bei den Datenschutzeinstellungen deaktivieren? Auswertung wer wessen Nachrichten/Dokumente/ Chats wie schnell liest/ antwortet) deaktvieren?)

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

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.

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.



© iStock

Für das gemeinsame Arbeiten an Dokumenten, können die Teilnehmer:innen ihren Desktop freigeben, 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 oder einer Konferenz sollte zu jedem Zeitpunkt für jede/n Teilnehmer:in ersichtlich sein.
- Anzeigen des Arbeits- bzw. Erledigungsstands der Kolleg:innen dienen nicht der Leistungs- und/oder Verhaltenskontrolle
- Keine automatisierte Freigabe des Status
- Deaktivierung der Möglichkeit, andere Nutzer:innen über Statusänderungen zu benachrichtigen
- Keine Standortangaben freischalten
- Auswertungsverbot für Analysen, deren Zweck es ist individuelles Verhalten zu vergleichen oder zu beurteilen

DELVE

Delve ist seit 2015 ein fixer Bestandteil von MS 365. MS bezeichnet Delve als „Dokumentenmanagementsystem". Sämtliche Aktivitäten, unabhängig davon über welche Apps sie laufen werden von Delve gesammelt – vorausgesetzt die Aktivitäten finden in MS 365 statt. Delve sammelt zusammengefasste Daten wie die

Anzahl der Nutzer:innen, Anzahl der Leser:innen und die Kommunikationshäufigkeit untereinander. Delve ist eine Schnittstelle zwischen den verschiedenen Apps. Die englische Bedeutung der App bedeutet sich in etwas zu vertiefen, etwas erforschen, ist also durchaus passend gewählt.

Delve ist als Suchfunktion geeignet (z. B. nach Stichwörtern quer durch alle Laufwerke, E-Mails, Fotos, Protokolle etc.), wofür allerdings ebenso Sharepoint [S. 60] genutzt werden kann. Delve bietet Nutzer:innen die für ihre jeweiligen Arbeitsaufgaben „passenden" Dokumente und Informationen automatisch an. Nutzer:innen können sich ein selbst definiertes „Board" anlegen, wo sie selbsttätig ihre Favoriten auswählen.
Delve sortiert sämtliche E-Mails, Kontakte, Termine, Präsentationen, Dokumente, Bilder etc. und man weiß nicht, welche Parameter dem Sortieren genau zugrunde liegen (z. B. nach den jeweiligen Bearbeiter:innen? nach Inhalt oder Schlagworten von Dokumenten? nach dem Zeitpunkt der letzten Bearbeitung?). Nach welchen Kriterien diese „Relevanz" beurteilt wird, beruht auf einer Microsoft-internen Berechnung und ist für Nutzer:innen nicht im Detail ersichtlich. Offengelegt ist, dass folgende Parameter einfließen: das persönliche Kommunikationsverhalten, die Häufigkeit von (gemeinsamen) Dokumentenaufrufen und -bearbeitungen (z. B. Excel) sowie Terminkalender und Notizen. Seit 2020 nennt MS diese Auswahl- und Präferenz-Funktionen bei Delve „künstliche Intelligenz".

Auch wenn MS zu Delve nicht sehr transparent ist, so sollte es zumindest seitens des Arbeitgebers/der Arbeitgeberin so weit als möglich versucht werden, indem die App in Schulungen dargestellt wird bzw. informiert wird, was sie kann – und was nicht.

Delve kann zwar abgeschaltet werden, erfasst werden Nutzer:innendaten aber dennoch über Graph [S. 38]. Durch das Deaktivieren von Delve ist die Aktivität anderer Nutzer:innen nicht mehr ersichtlich und andere Nutzer:innen sehen die eigene Aktivität ebenso wenig. Auch Systemadministrator:innen können bei Delve nur begrenzt technische Einstellungen vornehmen.

In einer Betriebsvereinbarung eines deutschen Konzerns wird die Funktionsweise von Delve beschrieben und deren Einsatz konkretisiert:

Informationen zur eigenen Person sind freiwillig und können jederzeit wieder gelöscht werden. Eingestellte Profilbilder zur eigenen Person werden unternehmensweit im Mitarbeiterportal angezeigt. Dies kann nicht auf bestimmte Bereiche beschränkt werden. Freiwillig eingestellte Informationen zur eigenen Person müssen einen dienstlichen Bezug aufweisen. Die Angabe rein privater Daten ist untersagt. Zusätzlich analysiert Delve die Art und Weise, an welchen Dokumenten, Dateien und Inhalten Sie und Ihre Kollegen wie oft arbeiten und zuletzt gearbeitet haben, wer dieselben oder ähnliche Themen bearbeitet und wer mit wem wie oft interagiert. Diese Funktion ist im Standard aktiviert und kann jederzeit vom User deaktiviert werden. Weder Sie noch Ihre Kollegen können dann Ihre Dokumentenempfehlungen und Aktivitäten mehr sehen, sondern nur noch Ihre Profilinformationen.

Es ist daher ratsam in der BV zu regeln:

- Freiwilligkeit der Verwendung von Delve
- Schulung
- Information der Beschäftigten über die Funktionen von Delve
- Freiwilligkeit vereinbaren
- Festlegen für welche Zwecke Delve verwendet wird (z. B. Suche nach verlorenen Unterlagen)
- Festlegen, wer Zugriff auf Delve bzw. Protokolle von Delve haben darf; streng reglementieren (z. B. Einsicht nur bei konkreten Verdachtsmomenten auf strafrechtlich relevantes Verhalten im Beisein des Betriebsrates) oder Zugriff nur auf eigenes Board erlauben und keinesfalls die Freigabe dieser Boards für andere Kolleg:innen

Delve wird ausschließlich zur Informationsverwaltung durch die Beschäftigten für sich selbst genutzt. Die Nutzung ist freiwillig. In den Schulungen wird auf die Möglichkeit zur Deaktivierung von Delve hingewiesen.

- Delve deaktivieren – und immer wieder nachprüfen, ob die Einstellung im Admin-Center auch aktuell ist ODER: Delve nur für eine möglichst kleine Gruppe von Administrator:innen aktivieren und mit diesen eine Geheimhaltungserklärung vereinbaren

Sollte es in Ihrem Arbeitsumfeld kritisch sein, dass Sie „Delve" verwenden (z. B. als Mitglied eines Betriebsrates, der Jugend- und Auszubildenden- oder der Behindertenvertretung oder als Beschäftigter im betriebsärztlichen Dienst), sollten Sie ernsthaft erwägen, „Delve" abzuschalten.

Im Sharepoint-Admincenter gibt es die Möglichkeit über die Einstellung > „Entdecken" im Menüpunkt > „Office" > *„Delve und verwandte Funktionen aktivieren/deaktivieren"*; die Gewerkschaft GPA rät zur Deaktivierung.

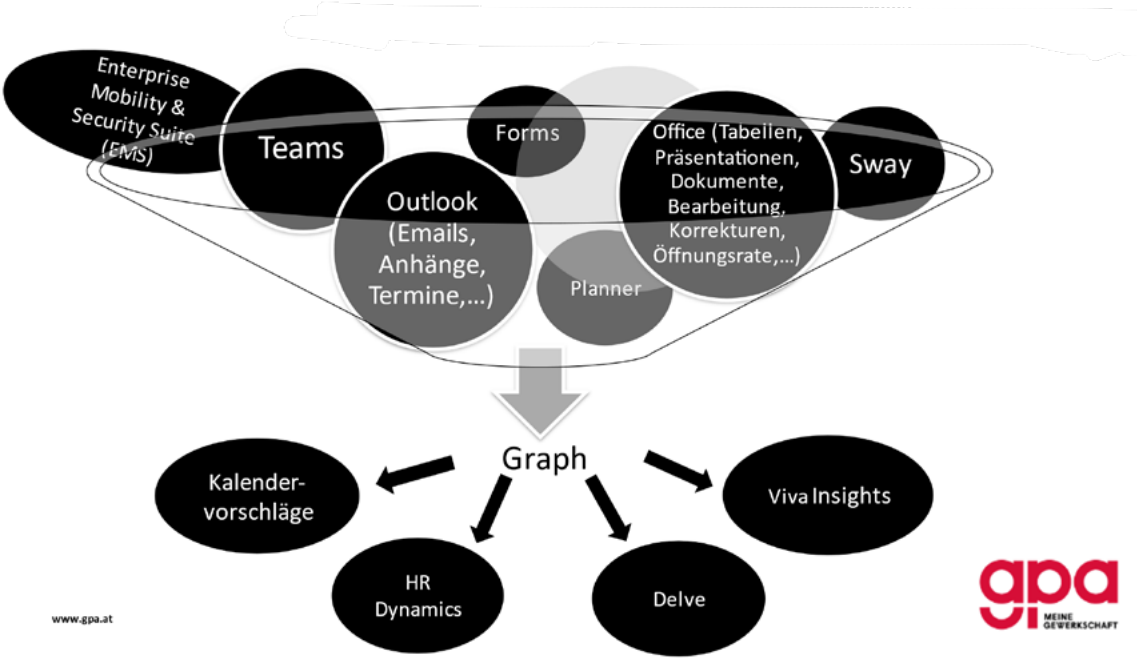
Eine Möglichkeit, ohne Delve zu arbeiten wäre es, MS 365 ausschließlich über firmeneigene Server auf den Stand-PCs laufen zu lassen, also „on premise". Auf der lokalen Desktop-PC-Version ist Delve nämlich nicht verfügbar. Wer Delve vermeiden möchte, könnte also ausschließlich mit der auf eigenen Servern laufenden Variante von MS 365 ohne Cloud-Services arbeiten. Einige Vorteile von MS 365 (z. B. geringer lokaler Speicher-Ressourcenverbrauch) gehen damit allerdings verloren.

GRAPH

Über Graph werden Nutzer:innen-Aktivitäten aus allen anderen Anwendungen zusammengeführt und ausgewertet. Graph stellt fest, wer, wie lange, wie häufig, mit welchen MS 365-Anwendungen arbeitet und mit wem, wie lange, wie häufig Kontakt besteht. Graph speichert Telemetriedaten nicht selbst sondern greift auf andere Anwendungen zurück und stellt die Ergebnisse wiederum in anderen MS-Anwendungen zur Verfügung.

Graph stellt Beziehungen zwischen den riesigen Datenmengen der MS 365 – Landschaft her. Bei Graph kann beispielsweise auch eine Schnittstelle eingebaut werden, die zur Sicherheit dient, indem sie „auffälliges Verhalten" feststellen. Ein solcher Security-Graph misst

FUNKTIONSWEISE VON GRAPH



Abweichungen von „normalen“ Verhaltensweisen auf den diversen Apps, stellt „auffälliges“ Verhalten unter Quarantäne und löst Warnungen aus.

Über Schnittstellen (Graph Connectors) können auch Apps außerhalb von MS 365 in die Auswertungen integriert werden.

Die permanente Datenerfassung durch Graph läuft immer im Hintergrund mit. Zwar kann man verhindern, dass die Auswertungen angezeigt werden (z. B. indem man Delve [S. 47] deaktiviert), doch verhindert man mit dem Abschalten nicht generell, dass Daten der Nutzer:innen verarbeitet werden. Technische Verhaltenskontrolle wohnt dem System von MS 365 per se inne.

Graph läuft immer im Hintergrund mit und kann nicht abgedreht werden.

Systemadministrator:innen könnten, auch wenn Nutzer:innen es nicht aktiv verwenden, das so genannte „Benutzeraktivitätsberichtsprotokoll“ einsehen. In der BV muss also auf organisatorischem Wege ausgeschlossen werden, dass diese Überwachung eingesehen oder ausgewertet wird oder gar negative Folgen für die Beschäftigten hat.

Für die BV zu regeln:

- Einstellungen so vornehmen, dass möglichst viele Daten in anderen MS 365-Anwendungen verborgen werden

- Allfällig vorhandene Schnittstellen (so genannte Application Programming Interfaces, API) oder selbst programmierte Abfragen (z. B. über Power Apps s S. 62) von Graph zu Programmen außerhalb von MS 365 möglichst unterbinden; braucht es welche, müssen sie genau definiert werden und dürfen nur für eindeutig festgelegte Programme genutzt werden und bedürfen der Zustimmung des Betriebsrates

- Das Erstellen eigener, zusätzlicher Auswertungen, Scripts oder Abfragen seitens der Administrator:innen unterbinden

Die API von MS Graph darf durch die Arbeitgeberin nicht genutzt werden.

VIVA

Diese App hat eine bewegte Geschichte. Erstmals 2015 unter dem Namen „Delve Organisational Analytics“ auf den Markt gebracht, kam sie in ähnlicher Form mit der App „Workplace Analytics“ bzw. „My Analytics“ 2017 für Firmenkunden zum MS 365-Paket hinzu. In Analytics wurde aus hochgeladenen Dateien, Beteiligung an Videokonferenzen, und ähnlichen Aktivitäten ein Produktivitätsscore für jede/n Nutzer:in berechnet. My Analytics wiederum gab aufgrund der Aktivitäten auf MS 365 persönliche Tipps zur Work-Life-Balance, Kontaktaufnahme. Die daraus kreierten, eher diffusen Auswertungen sorgten für Diskussionsstoff. Seit 2021 bedient die App „Viva“ ähnlich gelagerte Wünsche (mitunter auch „Delve“ [s S. 47] oder „Dynamics“ [s S. 53]).

Viva ist eine Analyse- bzw. Empfehlungs-App, die dazu dient, die persönliche Arbeitsweise der Nutzer:innen zu erkennen und durch die Analyse ebendieser helfen soll, „noch produktiver“ zu arbeiten. Viva besteht aus mehreren Paketen und wird vor allem von Seiten des Personalmanagements genutzt.

Auf **Viva Learning** werden Lerninhalte aus dem gesamten Unternehmen oder auch externe Angebote für die Kolleg:innen (mitunter individuell angepasst) bereitgestellt und an das individuelle Arbeitsprofil angepasst empfohlen.

Viva Insights fordert auf: „Entdecken Sie Lösungen, die Effektivität und Wohlbefinden im täglichen Arbeitsfluss stärken.“ Wer das Feature verwendet, erhält Tipps gegen Entgrenzung der Arbeitszeit, für „Fokuszeiten“, zu Kolleg:innen mit denen man Kontakt aufnehmen sollte, welche E-Mails man bevorzugt behandeln sollte usw. Der/ die Nutzer:in erhält von Viva Insights auf das persönliche Verhalten abgestimmte Vorschläge zum effizienteren Arbeiten oder zum besseren Wohlbefinden. Ein Schönheitsfehler bei Viva Insights war dessen Datenübermittlung in die USA. Diesen hat

Microsoft behoben und beteuert: „Für neue Kunden von Viva Insights ist seit dem 1. Mai 2022 eine Speicherung der Daten aller Funktionen in der Europäischen Union möglich. Die Daten bestehender Kunden werden bis 31. Dezember 2022 in ein europäisches Rechenzentrum in den Niederlanden transferiert."[18]

Viva Connections ist als eine Art personalisiertes „Schwarzes Brett" für die wichtigsten Informationen eines Unternehmens konzipiert.

Viva Engage ist als Austauschmedium gedacht, wo sich Kolleg:innen persönlich mit ihren Vorschlägen einbringen können.

Auf **Viva Goals** werden Ziele und deren Erreichen dargestellt, und automatisiert auf Basis der bisher von MS 365 gesammelten Informationen verglichen.

Auf **Viva Sales** schließlich werden Kund:innen-Informationen zusammengetragen und daraus Empfehlungen abgeleitet, beispielsweise welche Kundin, welcher Kunde demnächst kontaktiert werden sollte.

Viva greift unter anderem auf Daten aus Outlook [S. 39] zu. Betriebsrätinnen und Betriebsräte berichten, dass die Funktion der Fokuszeiten gerne von den Kolleg:innen genutzt werden, um so im Kalender für die anderen blockiert zu sein und in Ruhe arbeiten zu können.

Viva kann die Beziehung zwischen Teams und deren Mitgliedern mit unterschiedlich starken 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".

Viva lernt mit, wer welche Vorlieben hat und entwickelt daraus die nächsten Tipps.

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

Kann kein Grund genannt werden, wofür man Viva einsetzt, spricht viel dafür, Viva nicht zu aktivieren!

Falls Viva verwendet werden soll wäre in der BV genau zu konkretisieren:

- Enge Zweckbindung; Wozu wird Viva eingesetzt (z. B. Angebote für Lerninhalte sehen, neueste Informationen sehen)
- Freiwilligkeit klären
- grundsätzlicher Verzicht der Nutzung personen- und kleingruppenbezogener Analysefunktionen (z. B. bei Wahrnehmung von Schulungsangeboten, Beteiligung am Schwarzen Brett etc.); ausschließlich Personengruppen, die mehr als zehn Individuen umfassen, zusammen dargestellt werden
- arbeitsrechtliche Maßnahmen, die auf Auswertungen von Viva basieren, für unwirksam erklären
- Updates vorab prüfen (siehe S. 32)

TODO

Mit ToDo kann sich jede/r Nutzer:in Listen erstellen. Je nach persönlichem Wunsch beinhaltet die ToDo-Liste zusammengefasst aus anderen Apps (z. B. Kalender, Planner, Teams) was zu tun ist, was mehr Übersicht bringen soll. Vor der Aktivierung von ToDo sollte man abklären, ob andere Apps für die Arbeitsorganisation besser geeignet sind (z. B. Planner).
Gesehen wird von Admin-Seite nur; ob die App verwendet wird, nicht was damit gemacht wird.

In einer BV empfohlen:

- Freiwillige Nutzung
- Ausschließlich persönliche Einsicht und Nutzung

18 https://news.microsoft.com/de-de/microsoft-viva-insights-bietet-datenspeicherung-in-europaeischen-rechenzentren/

STREAM

Auf diesem Videoportal können firmenintern Videos hochgeladen werden. Informationen werden damit unter den Beschäftigten verbreitet. Stream ist für interne Kommunikation und Schulung gedacht.

Stream liefert keine personenbezogenen Verbindungsdaten. 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.

In der BV festgelegt werden sollte:

- Freiwilligkeit, etwas hochzuladen
- Zweckbestimmung (z. B. Schulungen ja, Weihnachtsfeier-Videos nein)
- Zustimmung der auf den Videos abgebildeten Personen einholen
- Speicherdauer
- Ausschließlich unternehmensinterne Nutzung und Ansicht der Videos

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. 39], Teams [S. 42]). Über die Anzeige des Status können andere Nutzer:innen erkennen, ob jemand gerade erreichbar ist oder auch, warum jemand nicht erreichbar ist (z. B. Urlaub).
Diese Information ist nicht nur für die Kolleg:innen ersichtlich, sondern auch MS stellt damit Berechnungen an und gibt – falls Viva verwendet wird – in Viva Insights [S. 50] Tipps, wie die Zeiteinteilung optimiert werden könnte.

Der Status wird auch automatisch über den Terminkalender bestimmt – das manuelle Rücksetzen kann man also getrost bleiben lassen.

Die Voreinstellungen können nicht auf selbst definierte Status abgeändert werden.

Die Funktion „Benachrichtigen wenn verfügbar" ist problematisch, da eine Nachricht an die Person, die dies anfordert, versendet wird, sobald die/der gewünschte Kollegin/Kollege seinen/ihren Status entsprechend ändert – mit dem kleinen Schönheitsfehler, dass die gewünschte Person nichts davon weiß und diese Benachrichtigung, auch wenn sie es wollte, nicht unterbinden kann. Ein SMS „Bitte ruf mich zurück" wäre vermutlich ausreichend und würde die gewünschte Person nicht einer heimlichen Überwachung aussetzen. Von der Verwendung der „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)
- historische Rückschau sowie Prognosen bevorstehender Status (z. B. Verfügbarkeit in einer Woche, Zeitsummen pro Monat,...) unterbinden
- 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. Eine historische Rückschau der Status-Zeiten (über 90 Tage hinaus) wird weder vom System vorgenommen, noch ist die Aufzeichnung und längerfristige Beobachtung zulässig.*

> *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.*

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.

PLANNER

Planner ist eine App zum Organisieren von gemeinsamer Projektarbeit. Im Planner können Projekte angelegt, Aufgaben verteilt und einzelne Schritte für alle transparent durchgeführt werden. Alle Team-Mitglieder sind automatisch berechtigt, im Planner Projekte zu erstellen und zu gestalten. Jede und jeder kann bestimmte Aufgaben nach selbst definierten Kategorien erstellen und bestimmte Personen den einzelnen Schritten zuordnen, sie sozusagen mit der Erledigung bestimmter Projektschritte beauftragen. Typische Elemente von Aufgaben sind Startdatum, Deadline, Status, Unteraufgaben, zugeordnete Personen, Anhänge.

Wird hier 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 sämtliche Anwendungen miteinander verknüpft sind.

Technisch gesehen können mit Planner auch gemeinsame Dokumente bearbeitet werden. Allerdings eignet sich Teams (siehe S. 42) wesentlich besser für diese Tätigkeit.
Planner bietet somit einen strukturierten Überblick über Projekte und stellt in einem Diagramm dar, was von den einzelnen Projektteam-Mitgliedern erledigt ist, was noch erledigt gehört, wer wann seine/ihre Aufgeben erledigt hat – oder auch säumig ist.

In der BV zu Planner sollte geregelt werden:

- Die Zwecke festlegen in Abgrenzung zu anderen Apps von MS 356, die ebenfalls zur Befragung und Prozessgestaltung verwendet werden können (z. B. Kalender, ToDo, Lists, Teams, Channels)
- Mitglieder mit Berechtigungen entsprechend der festgelegten Zwecke beschränken (z. B. Projektgruppe)
- Keine Vergleiche zwischen Projektgruppen oder gar Personen zulassen
- Festlegen, wer Aufgaben und Termine an andere (verpflichtend) verteilt
- Festlegen, ob auch private Nutzung einfließen soll (z. B. belegte Termine)
- Festlegen welche Kategorien gebildet 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 versäumt werden?)
- Keine arbeitsrechtlichen Konsequenzen aus Planner-Inhalten (z. B. versäumte Deadline, nicht-erledigte Aufgabe) ableiten

DYNAMICS

Dynamics ist ein eigenes Programm außerhalb des MS-Universums für die Personalverwaltung, Human-Ressource, Lohnverrechnung, elektronischer Personalakt, Arbeitszeiterfassung, Dienstreisen, Urlaub, Rekrutierung und Kündigung, Qualifikation, Weiterbildung, Self-Service für die Beschäftigten, HR-Reports ..., für all das bietet Dynamics 365 eine eigene Anwendung. Bislang ist Dynamics (noch) bloß vereinzelt in Österreich in Verwendung, was vermutlich daran liegt, dass in der Personalverwaltung klare rechtliche Vorgaben einzuhalten sind, die sich von denen im Mutterland von MS deutlich unterscheiden. Dynamics kann in die MS 365-Landschaft eingebunden werden.

Dynamics hat ein breites Anwendungsgebiet. Es kann genutzt werden für das Verkaufs- und Kunden(-beziehungs-)management im Vertrieb, zum Recruiting, On- und Off-Boarding in der HR, für die Finanzberichterstattung oder auch die Buchhaltung.

MS „Customer Service“ ist ein Teil von MS 365 Dynamics und bietet an, dass aus Social Media stammende

Daten (z. B. Posts auf Facebook, Beurteilungen auf Fanseiten 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. Diese App verarbeitet Informationen aus Social Media, die spätestens, wenn das private Umfeld oder die Beschäftigten selbst zu Kund:innen des Unternehmens werden in die Privatsphäre reichen, und ist daher besser zu unterbinden.

In einer BV ist zu regeln:

- Klare Zweckbegrenzung
- Zugriff für Auswertungen, Auszahlungen und Aktualisierungen ausschließlich für die Personal- und Finanzverantwortlichen
- Zugriff zur lesenden Kontrolle für die Beschäftigten auf ihren eigenen Account (ev. ein Employee-Self-Service; MitarbeiterInnen-Portal einrichten ohne fremde Zugriffsmöglichkeit)
- Einsicht für den BR zur Kontrolle
- Auswertungen grundsätzlich ohne Personenbezug (z. B. Lohnsummen, Verkaufssummen, Prozentangaben zu leistungsorientierten Lohnbestandteile, Überstundensummen etc.); für personenbezogene Auswertungen (neben den gesetzlich vorgeschriebenen) Anlassfälle definieren
- Prognosen (z. B. Verkaufstrends) immer ohne Personenbezug
- Keine Verwendung besonderer Datenkategorien (z. B. Gesundheit, sexuelle Orientierung etc.)
- Kein Profiling! (d.h. erstellen automatisierter Profile auf Basis von Dynamics-Daten)
- Keine automatisierte Entscheidungsfindung! (d. h. Automated Desicion Making (ADM) wie z. B. wer wird befördert/gekündigt)
- Keine großflächige Überwachung der Beschäftigten!

FORMS

Forms ist eine einfach zu handhabende Software für das Erstellen von Umfragen. Die App kann für alle möglichen Interessen eingesetzt werden, um beispielsweise regelmäßig etwas über das Betriebsklima zu erfahren, um einen Termin zu koordinieren oder auch für die um Wünsche an die Betriebsratsarbeit zu erfragen.

Beim Versenden der Umfrage können Links oder QR-Codes als Zugang mit verschickt werden, was für Befragte ohne MS 365 Zugang die Teilnahme ermöglicht.

Eine Umfrage zu erstellen ist eine komplexe Angelegenheit. Die Themen müssen einen Bezug zum Arbeitsleben haben. Die Fragen sollen gut verständlich und neutral formuliert sein. Die Auswertung sollte Mindeststandards an Verlässlichkeit und Repräsentativität für das Unternehmen erfüllen. Daher ist eine Schulung jener Arbeitnehmer:innen, die Umfragen erstellen und auswerten, sinnvoll ohne die es an der für Befragungen erforderlichen Knowhow und Sensibilität mangelt.
Haben sämtliche Beschäftigten Zugang zu Forms, kann es auch passieren, dass viele Kolleg:innen es „ausprobieren", damit „spielen" wollen, dass beliebige Umfragen erstellt und verschickt werden und Beschäftigte einen Gutteil ihrer Arbeitszeit mit dem Erstellen, Beantworten, Korrigieren, Auswerten und Interpretieren von Befragungen beschäftigt sind. Es liegt auf der Hand, dass dem ein Riegel vorgeschoben werden sollte.

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 im Sinne eines effizienten Projektmanagements anzuraten.
Das mit den **Antworten** mitgelieferte Protokoll auf 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 Antworten gehören zwar transparent gemacht aber nicht individuell dargestellt, sondern nur in Prozent, also **statistisch**. Wäre eine Umfrage auf Forms namentlich, bietet sie keinen Schutz der Privatsphäre. Wann eine namentliche

Forms-Befragung zweckdienlich sein kann, muss vorab genau angesehen und beurteilt werden.

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 (zB Genehmigungsprozess, Rücklauffrist...)
- Speicherfristen
- Einstellung „Namen erfassen" standardmäßig deaktivieren
- Einstellung „Einzel-Ergebnisse anzeigen" standardmäßig deaktivieren
- Ergebnisse standardmäßig nur anonym zulassen und keinesfalls Arbeitsleistung daraus ableiten
- Ergebnisse in einem verschlüsselten Bereich ablegen
- Ergebnisse im Betrieb (statistisch) kommunizieren
- Auswirkungen der Befragung vorab auf die angegebenen Ziele einschränken
- Aufbewahrungsdauer festlegen („retention policy")

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 individuell gestaltbarer Bereich zum Ablegen von Dateien aller Art. Wer „Dropbox" nutzt, dem wird diese App bekannt vorkommen. Auf OneDrive können sämtliche Dateiformate (z. B. Texte, Musik, Fotos etc.) in selbst definierten Ordner-Systemen abgelegt und 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 die Dateien auch gemeinsam angesehen und auch mit einer anderen MS-App (z. B. Office S. 38) bearbeitet oder über eine MS App (z. B. Teams S. 42) geteilt werden.

Eine Empfehlung für derartige externe Speicher kann nicht ausgesprochen werden, da sie sich derzeit fast immer in den USA befinden und es dadurch zu Problemen mit Datensicherheit (s. Netz- und Informationssicherheitsgesetz, NISG), Privatsphäre (s. Datenschutzgrundverordnung DSGVO) und Dateneinsicht durch US-amerikanische Geheimdienste (s. Cloud-Act) kommt.

Ebenso wenig kann die Nutzung des Gratis-Angebots von OneDrive [S. 55] nahegelegt werden, da sich MS hier vorbehält, sämtliche Telemetriedaten mitzulesen.

Administrator:innen haben nicht automatisch Zugriff. 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 allerdings im „Compliance Manager" (s S. 66] von MS 365 umgangen werden – sollte OneDrive über eine andere MS 365 App eingehängt worden sein. Dabei wird für den/die Besitzer:in von OneDrive ein Link zum Admin gelegt.)

Nutzer:innen, die die entsprechende Berechtigung für die „Websitesammlungsadministratoren" haben, können nachprüfen, ob und wer sich bei ihrem OneDrive Zutritt verschafft hat. Dazu kommt man über die im Menüpunkt „Berechtigungen" der „Anwendungsverwaltungen". Außerdem tauchen sämtliche Zutritte auch im „Log- Protokoll" des Menüpunkt „MS Purview Security & Compliance" auf. Auf diesem Wege könnte man allfällige unliebsame Einsichtnahmen überprüfen.

In einer BV empfehlenswerte Regelungen:

- Regeln für welche Dokumente OneDrive verwendet wird (z. B. keine Personalakten) – besonders in Abgrenzung 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 das kontrolliert wird.

- Zugriff regeln (Wer darf Einsicht nehmen? Wer darf im Abwesenheitsfall als Vertrauensperson Dokumente aus OneDrive sehen? Gibt es Gruppen-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

- Haftung klären falls wichtige Dokumente „verschwinden" (ev. zusätzlich Data Loss Prevention [S. 69] in Betrieb nehmen)

- Freiwilligkeit vereinbaren

MS verlangt nicht zwingend, dass sämtliche Texte, Bilder oder Sprachaufnahmen im MS-eigenen Speicher OneDrive abgelegt werden. Es könnten auch unternehmensfremde Apps genutzt werden (z. B. Dropbox, GoogleDrive oder das Citrix-System ShareFile). Diese Apps könnten an MS „angedockt" werden.

VISIO

Visio wurde von MS 1999 gekauft. Es ist also bereits lange Teil der MS 365 Produkt-„Familie" und gut kompatibel, muss aber eigens gekauft werden.

Mit Visio werden Grafiken erstellt, technische Zeichnungen angefertigt, Diagramme arrangiert, Prozesse visuell abgebildet und exportiert. Mehrere Personen können an einem Bild arbeiten.

© iStock

In einer BV zu regeln ist

- Zugriffsregelungen; Wer darf welche Diagramme sehen/bearbeiten/weiterleiten? Was darf wohin exportiert werden?
- Keine Leistungskontrolle

SKYPE

Skype hat ein bewegtes Leben hinter sich. Von 2010 bis 2015 trug die Echtzeitkommunikation von MS den Namen „LYNC". Den „Kommunikations-und-Tratsch-Vorgänger" von Skype, den „Live Messenger" gibt es seit 2013 nicht mehr. Doch auch für Skype ist seit 2017 klar, dass es nicht mehr lange leben wird. 2021 geht Skype in Teams [S. 42] über.

Regeln zum Skypen sollten mit den Regeln für das Video-Telefonieren in Teams [S. 42] jedenfalls in Einklang stehen.

Beim Chatten mittels kurzen Textnachrichten sollte generell Folgendes geklärt sein:

- Möglichst Freiwilligkeit festlegen
- Möglichst festlegen, welche Inhalte kommuniziert werden (z. B. Terminabsprachen) Festlegen, dass keine Arbeitsanweisungen oder Arbeitszeitänderungen via Skype erfolgen
- Zugriffs-, Kommentar- und Änderungsgrundsätze klären (wer darf welche Inhalte mitlesen/ ändern/ kopieren/ weiterleiten?)
- Löschfristen für Chats festlegen

YAMMER

Über Yammer wird geplaudert, es werden Bilder ausgetauscht, es ist ein betriebsinternes „social network". Man könnte es auch als „innerbetrieblichen Bassenatratsch" bezeichnen.

In Yammer erstellen die Beschäftigten oder auch Kund:innen und Geschäftsparter:innen persönliche Profile. Die Gruppen können anhand ihrer jeweiligen Qualifikationen koordiniert werden. Relevante Personen, Inhalte und Unterhaltungen können gefunden werden.

In Yammer können „einflussreiche" Arbeitnehmer:innen ermittelt werden, wobei nicht ganz klar ist, welche

Parameter herangezogen werden um dieses „Label" zu vergeben.

Nachdem die Verwendungszwecke, denen von MS Teams [S. 42] (bzw. außerhalb der MS-Welt denen von Facebook oder Xing) sehr ähnlich sind, ist anzunehmen, dass auch dieses Programm ein Ablaufdatum hat. Mittelfristig wird Yammer vermutlich in Teams aufgehen.

Wird Yammer in der Cloud verwendet und ist kein SharePoint im Betrieb eingerichtet, auf dem Chats und hochgeladene Dateien gespeichert werden können, stehen im EU-Raum einige Anwendungen nicht zur Verfügung (z. B. Dateianhänge speichern, Nutzer:innen nehmen an externen Yammergruppen teil etc.; Stand Februar 2023). Das liegt vermutlich daran, dass die Yammer-Daten in den USA gespeichert werden, was aufgrund der DSGVO Probleme aufwirft.

Chats, Aufnahmen und Uploads werden meist aber nicht in Yammer selbst sondern auf Sharepoint, also auf Unternehmensebene gespeichert. Das bringt den Effekt mit sich, dass mitgelesen werden kann. Ein Auswertungs-, Benachteiligungs- und Beweisverwertungsverbot werden daher in diesem Fall äußerst wichtige Bestandteile der Betriebsvereinbarung.

Bei Yammer sollten folgende Punkte in der BV klargestellt sein:

- Freiwilligkeit
- Freiwilligkeit für die Erstellung eigener Profile
- zu kommunizierende Inhalte festlegen (z. B. keine Krankmeldungen, keine Fahrtroutenänderungen, keine Schichtpläne etc.)
- Zugriffe für einen eingeschränkten Personenkreis (nicht nach dem Prinzip „alle sehen alles")
- Zeitnahes Löschen vereinbaren
- Zuständigkeit für Löschen der Chats vereinbaren (IT? Gruppenleitung? einzelne Nutzer:innen?)
- Auswertungs- und Benachteiligungsverbot
- Präsenzstatus ausschalten
- „Lob" bzw. dessen Auswertungen und Vergleiche ausschalten
- Schlüsselwortüberwachung ausschalten
- Festlegen ob externe Nachrichten/Chats inkludiert werden

SPRACHASSISTENZ

Was „Alexa" für Amazon und „Siri" für Apple, das ist „Cortana" für Microsoft – eine Sprachassistentin. Zwar wird der Name von MS selbst kaum verwendet, doch sind Spracherkennungsfunktionen in einigen Apps integriert. Also gilt: es muss nicht Cortana draufstehen, damit Spracherkennung drinnen ist.

Mit Cortana können MS 365-Apps gesteuert werden. MS beschreibt die App Cortana so: „Ihre persönliche Produktivitätsassistentin, bietet KI-gestützte Erfahrungen, um Zeit zu sparen und die Aufmerksamkeit auf das Wesentliche zu konzentrieren. (...) Cortana wurde entwickelt, um Features bereitzustellen, die Daten wie E-Mails, Dateien, Chats usw. sicher verarbeiten." Cortana hatte aber bislang, verglichen mit den anderen Freundinnen aus der Runde der Sprachassistentinnen eher bescheidenen Fan-Kreis. 2019 wurde Cortana für Privatnutzer:innen von Android- und Apple-Handys vom Markt genommen. Ein Update von Mai 2020 soll Cortana wieder Auftrieb verschaffen, indem einige zusätzliche sprachgesteuerte Features eingeführt werden (z. B. Termine, Erinnerungen, Aufgaben aus der To-Do-App, Abfrage über die MS-eigene Suchmaschine Bing).

Die Spracherkennung kann E-Mails auf Sprachbefehl verschicken oder nach Diktat schreiben, Dokumente suchen, Termine abfragen, Sprache in Text transkribieren etc. Ich diktiere: „Dieser Satz wird nun gesprochen, wobei die Diktierfunktion bei MS Word zum Einsatz kommt. Diese Broschüre könnte also auch per Office-Diktat ‚geschrieben' werden. Das funktioniert erstaunlich gut."

Beim Einsatz von Sprachassistenz wäre zu klären:

- Zwecke
- Freiwilligkeit sollte jedenfalls ein Grundprinzip bei der beruflichen Verwendung von Sprachassistenten sein
- Genaue Information an die Beschäftigten, dass der Sprachassistent aufnimmt, Daten speichert, Daten analysiert, mit anderen Anwendungen verknüpft ist

SWAY

Bei Sway handelt es sich um eine App für Präsentationen. Wer „Prezzi" kennt, wird mit Sway gut zurechtkommen. Videos, Text in verschiedensten Formatierungen sowie auch gesprochene Texte, 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, Produkt-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.

MS gibt zu, dass als Speicherort die USA zum Einsatz kommt. Solange das nicht geändert ist, sollte Sway nur für sehr allgemeine Darstellungen gewählt werden.

In einer BV wäre zu klären:

- Speicherort
- Verwendungszweck (z. B. betriebsinterne Lehrmaterialien)
- Berechtigungskonzept (wer darf hochladen, ansehen, löschen, verändern?)
- Löschfristen

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 auch innerhalb der unternehmensinternen Apps von MS 365 – wenn man das möchte. Bing verwendet also für den Suchalgorithmus auch das, was firmenintern hochgeladen wird (z. B. auf Sharepoint). Hat man andere Suchfunktionen mit denen (verloren geglaubte) Informationen wiedergefunden werden, ist Bing eigentlich nicht erforderlich.

Bing heißt die Nutzer:innen ganz persönlich willkommen und zeigt den eigenen Kalender, die anstehenden Aufgaben, den Aktivitätenbericht – wenn man das möchte (Stand: zweites Halbjahr 2022). Wenn man das nicht möchte oder zu diesem Zweck bereits andere Apps in Verwendung sind [s Viva S. 50], sollte man die Suchmaschine abschalten.

In den Einstellungen der Administrator:innen gibt es die Frage „Ihrer Organisation die Verwendung von Microsoft Bing Search gestatten". Sollte firmenintern kein spezifischer Zweck für die Verwendung von Bing vorliegen, kann diese Frage deaktiviert bleiben.

ADMIN-APPS

SHAREPOINT

SharePoint ist ein zentraler Dienst von MS, der ähnlich wie ein eigener Server, eine eigene Plattform für das gesamte Unternehmen zur Verfügung steht. Über SharePoint können beliebig viele und beliebig große weitere Seiten eingerichtet werden (z. B. Datei-Sammlungen, Communities, Mailboxen, Workflows, Telefonverzeichnis, Seiten, aktuelle Informationen, Kalender, Report etc.). Das Suchen nach Videos/ Personen/ Dateien funktionieren genauso über SharePoint, wie das Speichern. Im Grunde ist SharePoint ein riesiges Content-Management-System (CMS), auf dem unterschiedlichste Formate eingehängt werden können. Je nachdem, was das Unternehmen gerne über SharePoint laufen lassen möchte, ist diese Plattform geeignet, die jeweiligen Erfordernisse bereitzustellen.

Nachdem SharePoint eine übergeordnete Plattform darstellt, auf der wesentliche Entscheidungen getroffen werden, sollte sie nicht von x-beliebigen Nutzer:innen eingerichtet werden können, sondern nur von ausgewählten, gut geschulten Entscheidungsträger:innen.

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

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.

In einer Betriebsvereinbarung wird aufzählend dargestellt, welche personenbezogenen Daten in SharePoint verwendet werden. Das schafft Transparenz und Vertrauen und ist nachahmenswert:

Neben den aus dem Active Directory 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 eines 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. Eine Leistungs- und Verhaltenskontrolle ist ausgeschlossen.*

In der BV sollte geklärt werden:

- Berechtigungskonzept; Wer hat welche Berechtigung? Wer darf die Seite einrichten? Wer darf administrative Änderungen vornehmen? Wer darf zugreifen? Wer darf Dokumente verwalten? Wer darf teilnehmen?

- Eindeutige Zwecke (z. B. Bibliothek, Dokumentenablage)

- Festlegen, welche Daten nicht auf SharePoint abgelegt werden sollen (z. B. mittels einer Datenklassifikation im „Security and Compliance Center", die ausschließt, dass Gesundheitsdaten auf SharePoint liegen)

- Festlegen wie viel Speicher für wen auf den jeweils zugänglichen Seiten zur Verfügung gestellt wird und die Nutzer:innen darüber informieren

- Schulungen für Anwender:innen (in denen z. B. darauf hingewiesen wird, welche Analyse erfolgt und wie sie bei Bedarf abgeschaltet werden kann)

> *Besitzer:innen/Owner sind für die Gestaltung der SharePoint-Seite, für das Rollen- und somit auch Zugriffskonzept, Löschung von Dateien etc. ihrer Seiten verantwortlich. Sie erhalten eigene Schulungen.*

- Einsichtsrechte für den Betriebsrat auf jede in SharePoint erstellte Seite, um die Einhaltung der BV zu überprüfen

- Allfällige, weitere eingebundene Apps und Schnittstellen müssen dargestellt werden und zweckgebunden sein, die Team-Mitglieder müssen informiert werden

- Nutzer:innenverhalten auf den einzelnen Websites darf analysiert werden sofern kein Personenbezug gegeben ist

- Löschkonzept

POWER BI & POWER AUTOMATE

Mit dieser „App-Familie" können eigene Auswertungen programmiert, eigene Skripts geschrieben werden, auch wenn man über keine speziellen IT-Sprachen oder Programmierkenntnisse verfügt. Die Daten, die in die selbst zusammengebastelten Apps einfließen stammen aus dem „Power Business Intelligence" (BI).

In Power Automate (vormals „MS Flow") können Berechtigte definierte Abläufe und Anwendungen programmieren, wobei auf verschiedenste MS 365 Apps zugegriffen wird (z. B. Organisieren von bestimmten E-Mail-Anhängen aus Outlook direkt in OneDrive; Warnung falls jemand unentschuldigt bei einer teuren Weiterbildung nicht erscheint; Benachrichtigung falls Kolleg:innen in einem Team-Chat ein bestimmtes Wort verwenden u.s.w.).

Apps, die nicht aus der Welt von MS stammen, können ebenso eingebunden werden (z. B. automatische Push-Mails in Outlook wenn bestimmte Personen etwas twittern, Wettervorschau um Termine im Freien zu planen oder Ähnliches). Die Problematik dabei ist, dass jene Personen, deren E-Mails, Nachrichten, Chats etc. in die Power App eingebaut werden, davon nicht automatisch etwas erfahren.

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

- *Eine Lizenz zur Nutzung von PowerAutomate und PowerApp 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

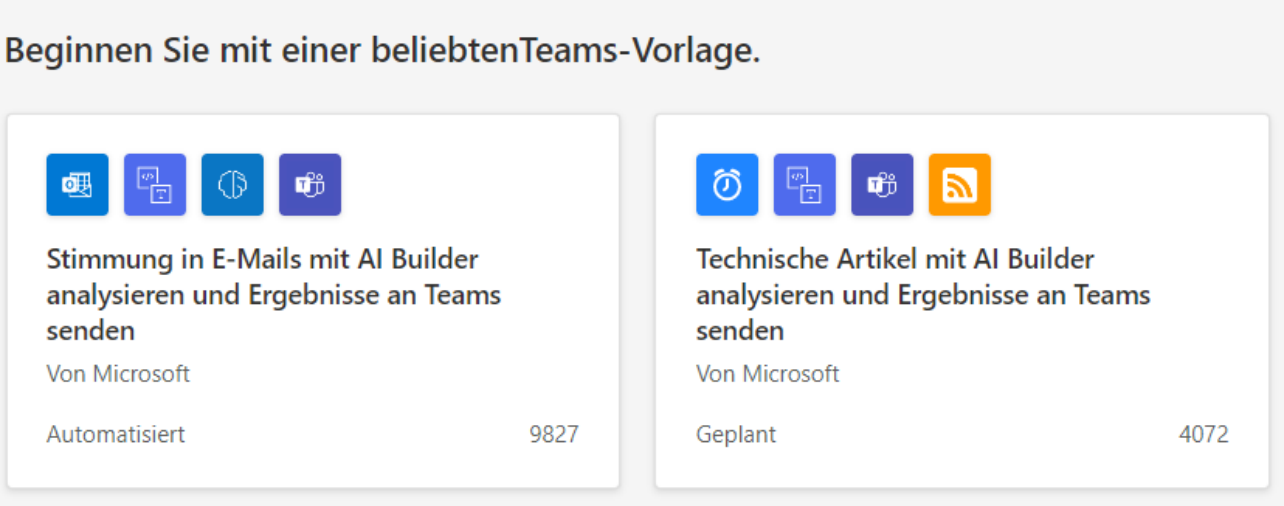
Auf Power Apps werden standardmäßig Optionen für Apps bereitgestellt (z. B. „Employee Engagement Survey", eine Umfrage zum Mitarbeiter:innen-Engagement, „Health Plan Selector", eine Krankenkassenleistungsübersicht des/der Arbeitgebers/in). Die meisten davon wurden erstellt, um dem Berichtswesen zu entsprechen, das nach US-amerikanischem Recht für Aktiengesellschaften vorgesehen ist.

Zusätzlich zu den Standards können eigene Power Apps mit Berichten aller Art zusammengestellt werden, ohne dass besondere Programmierkenntnisse erforderlich sind – und ohne dass die betroffenen Beschäftigten, deren Daten herangezogen werden, von den Berichten erfahren.

Power Apps können für eine Vertriebsanalyse, Analyse der IT-Auslastung oder das Festlegen von Arbeitsaufgaben verwendet werden. Sollten Power Apps allerdings Entscheidungen treffen, die ohne weiteres menschliches Zutun entstehen (sogenanntes „Automated Desicion Making" ADM) und die schwerwiegenden Auswirkungen haben (z. B. Diskriminierung, Herabsetzung oder Entzug von Boni, Versetzung, Kündigung) so ist das rechtlich unzulässig.

Es kann „Künstliche Intelligenz" in die Auswertungen einfließen, die dann beispielsweise eine effizientere Vorgehensweise empfiehlt – oder auch befiehlt. (z. B. Wer im Außendienst Kund:innen öfter telefonisch kontaktiert, erzielt einen höheren Umsatz und daher wird empfohlen, die Kund:innen öfter zu kontaktieren.) Neulich bot MS 365 an, mittels der KI zu analysieren, in welcher Stimmung jemand gewesen sei, als er/sie ein E-Mail verfasst hat.

„KÜNSTLICHE INTELLIGENZ" IN DER TEAMS-APP



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:

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

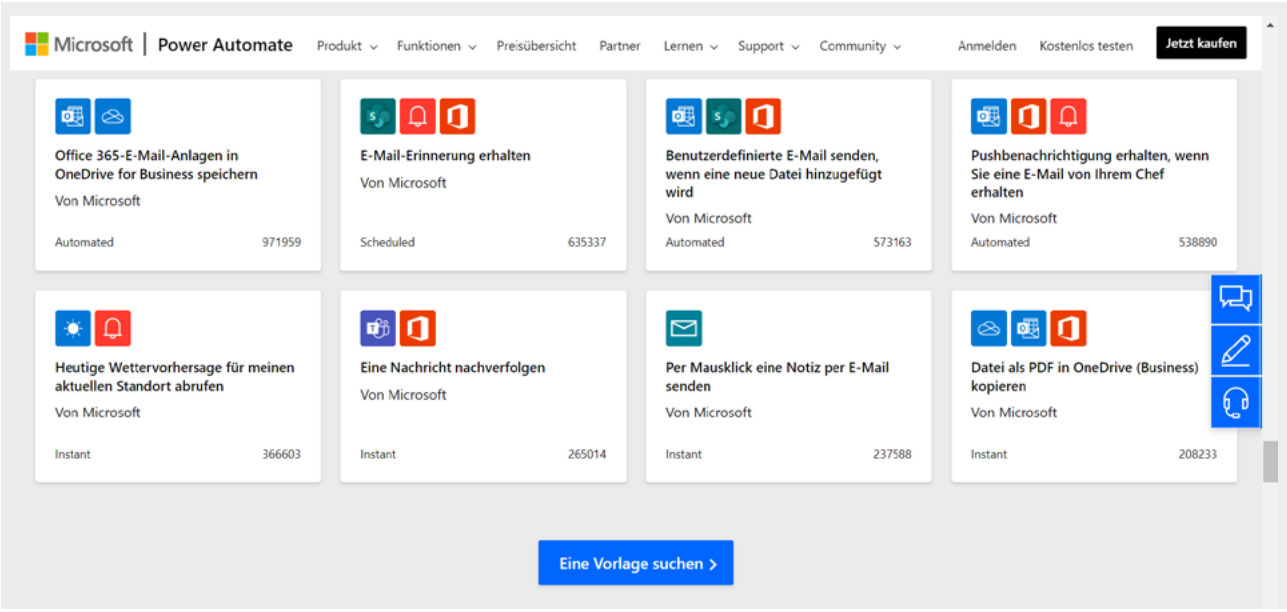
POWER VIRTUAL AGENT

Das ist der Chatbot von MS 365. Mit diesem Textprogramm lassen sich relativ einfach Unterhaltungen erstellen und führen. Gedacht ist die Funktion zur Kommunikation mit den Kund:innen.

Zu regeln ist:

- Wer erstellt die Bots?
- Wer hat Zugriff auf die Inhalte von Unterhaltungen?
- Wer beantwortet allfällige Anfragen bzw. an wen wird weitergeleitet?
- Welche Schulungen sind vorausgesetzt, damit der Power Virtual Agent verwendet werden darf?
- Was wird ausgewertet?
- Wann werden Unterhaltungen wieder gelöscht?

MÖGLICHKEITEN FÜR PERSÖNLICHE PROGRAMMIERUNG



EXCHANGE

Exchange ist wohl der meistgenutzte E-Mail-Server. Auf Exchange werden E-Mails und Kalender verwaltet. Posteingangsregeln, Vertretungsregeln, Weiterleitungen etc. werden über Exchange eingestellt. Auf Exchange werden beispielsweise das firmenweite Adressbuch angelegt, E-Mail-Listen verwaltet, Einsichtsrechte vergeben. Auf Exchange wird also sämtliche Aktivität in Outlook geregelt.

In den 2010er Jahren wurden vermehrt Server in Europa eingerichtet.

Sämtliche Kalender und E-Mails des Unternehmens können über Exchange synchronisiert werden und mithilfe der entsprechenden App „voneinander lernen". Der Kalender „lernt" beispielsweise, dass während eines Flugs keine E-Mail empfangen werden können, dass Besprechungen mit bestimmten Teilnehmenden länger dauern als geplant etc. Kurz: die Kommunikationsgewohnheiten der Nutzer:innen analysiert hinsichtlich ihrer Prioritäten, ihrer Lese- und Antwortgeschwindigkeit etc. Auf dieser Analyse aufbauend, können dann weitere Regeln erstellt werden – das Exchange „lernt".

Regeln für den Umgang mit E-Mails zu erstellen, ist eine empfehlenswerte Vorgehensweise, um die Speicherdauer zweckmäßig zu gestalten und die „Lebensdauer" von E- Mails, Kalendereinträgen, etc. möglichst kurz zu halten gemäß dem Prinzip der Datenminimierung. Allerdings können diese Regeln auch eingerichtet werden, um E-Mails automatisch in ein anderes Postfach weiterzuleiten. Wenn dies im Hintergrund so eingerichtet wird, merkt es der/die Empfänger:in nicht und hat auch keine Chance, diese Weiterleitung zu entdecken. Was im Fall von Spam-E-Mails, also unerwünschter Post, eine nützliche Vorgehensweise ist, entpuppt sich bei anderen E-Mail-Weiterleitungen als untragbar. Es ist technisch nicht möglich, eine automatische E-Mail-Weiterleitung in Postfächer anderer Kolleg:innen über Exchange zu verhindern – bleibt folglich nur ein Verbot derselben per Betriebsvereinbarung.

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.

Im Admin-Center von Exchange kann für Postfächer, die auf Exchange eingerichtet wurden, definiert werden, wie lange gelöschte Elemente aufbewahrt werden.

Falls auf Exchange [S. 64] relevante Sicherheitseinstellungen vorgenommen werden (z. B. Umgang mit Sicherungskopien, automatische Speicherung), müssen die Beschäftigten darüber informiert werden.

In einer BV sollte insbesondere geregelt werden:

- Wer darf was?
- Welche Auswertungen werden standardisiert personenbezogen vorgenommen? Der Zugriff auf derartige Auswertungen sollte jedenfalls wenigen Personen (z. B. in der IT-Abteilung) vorbehalten sein.
- Auf BackUps (also ältere Dateiversionen) sollten ausschließlich Administrator:innen zugreifen können
- Stehen die Regeln für Outlook [S. 39] und Teams [S. 42] mit denen von Exchange in Einklang?
- Sind „lernende" Apps an Exchange angehängt; wenn ja, mit welchem Zweck?

PURVIEW DEFENDER (VORMALS: ADVANCED THREAT PROTECTION (ATP))

Seit dem Update von Jänner 2023 tragen die meisten Safety-&-Security-Apps den „Vornamen" Purview; diese Bezeichnung wurde den Sicherheitsprogrammen vorangestellt. Der MS Purview Defender dient, wie der Name unschwer erkennen lässt, der Schadensabwehr. Im Admin-Infocenter zu Defender werden die Regeln festgelegt, wann ein Alarm ausgelöst wird. Hier wird protokolliert, was vor und nach einem Alarm im gesamten Unternehmen vorgefallen ist. Hier kann eine Reaktion auf einen Alarm festgelegt werden (z. B. Passwörter zurücksetzen, Anmeldevorgänge blockieren, E-Mails

löschen etc.), sodass einem abermaligen, ähnlichen Ereignis vorgebeugt wird. Die im Defender vorhandenen Abwehrmaßnahmen müssen von den zuständigen Administrator:innen genehmigt werden.

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

Der Defender kann in gewisser Weise als Schulungstool eingesetzt werden. Dabei werden Bedrohungs-Szenarien anhand der vorhandenen Daten entwickelt, woraufhin der Defender ein Programm entwickelt, das einen Angriff simuliert. Öffnen beispielsweise Beschäftigte Attachments von Fishing-Mails, verschickt Defender ein selbständig entwickeltes Fake-Mail an bestimmte Beschäftigte damit diese ihre Reaktion verbessern können. Somit sollen die Nutzer:innen über diese „Schulung" lernen, zukünftigen Schaden zu vermeiden. „Sensibilisierung und Training" nennt MS dieses Vorgehen.

Für den Defender ist zu regeln:

- Welche Vorgänge eine Benachrichtigung bzw. einen Alarm auslösen, also: welche Richtlinien hinterlegt sind
- Welche Aktivitätsprotokolle wie lange aufbewahrt werden
- Wer die Protokolle sehen darf
- Wie mit ad-hoc Kontrollen/ Tests zum Sicherheitsverhalten 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.)
- Information der Beschäftigten
- Beteiligung des BR

E-DISCOVERY

Im MS Purview (wie seit dem Update von Jänner 2023 die meisten Safety-&-Security-Programme genannt werden) E-Discovery wird automatisiert, verdachtsunabhängig und revisionssicher jeder Sicherheitsvorfall gespeichert – vorausgesetzt es wurde ein solcher Fall angelegt.

Für Datenforensiker:innen ist das E-Discovery Gold wert, da sämtliche Kommunikationsverläufe und -inhalte nachvollzogen werden können. MS wirbt damit, dass dieses Tool für juristische Zwecke verwendet werden kann, da es vor (späteren) Manipulationen schützt und nennt als Beispiel „Rechtsstreits mit Mitarbeiter:innen", womit auch schon offenbart ist, dass es sich zur Überwachung der Beschäftigten bestens eignet.

Zugangsberechtigte können eigens „Fälle" anlegen und so nach eigenen Kriterien Durchsuchungen durchführen. Das E-Discovery kann auch dem simplen Wiederauffinden von Texten, Bildern, Chats, Tabellen, u.s.w. dienen. Wenn (problematische) Inhalte von Texten auch anderwärtig gesucht werden können, generell kaum vorhanden sind oder kein Problem darstellen, kann diese App auch deaktiviert bleiben.

Für ein schlichtes Auskunftsbegehren von Betroffenen eignet sich das E-Discovery weniger, da es zu umfassend und unübersichtlich ist.

In den meisten Branchen und Betrieben sind die üblichen Archive und Speicherorte ausreichend, weshalb man den extra Behalte-Bereich vermutlich nicht unbedingt braucht.

In einer BV sollte geregelt werden:

- Zugriffsbeschränkungen (z. B. Forensiker:innen)
- eingeschränkte Zwecke (z. B. Gerichtsprozesse/ Gerichtsgutachten, schwere Sicherheitsattacken, Kund:innenbeschwerden)
- Verbot der anlasslosen Nutzung

- Verbot einen Fall zur BR-Kommunikation anzulegen
- Schweigepflicht für jene, die einen Fall im E-Discovery erstellen, solange der Fall aufrecht ist
- Speicherdauer
- Stichprobenartige Zutritte für den Betriebsrat, um die Einhaltung der BV überprüfen zu können bzw. um sich allfällig angelegte „Fälle" begründen und erläutern zu lassen

COMPLIANCE MANAGER (VORMALS: SECURITY AND COMPLIANCE CENTER)

Im Compliance Portal (bzw. in manchen Linzenzmodellen auch „Suite" genannt) von MS Purview (wie seit dem Update von Jänner 2023 der „Vorname" der meisten Safety-&-Security-Apps lautet) werden die Sicherheitsrichtlinien für sämtliche MS 365-Apps festgelegt. Die Administrator:innen können hier die Funktionsweise der Sicherheitstools testen, analysieren, kontrollieren oder (strenger) gestalten. Hier werden Speicher-Richtlinien festgelegt (die sogenannten „Retention Policies" z. B. wie lange Überwachungsprotokolle aufbewahrt werden). Hier wird festgelegt, wer sich wie und wo anmelden darf.

Ziel von MS Security ist es, Viren und andere Angriffe zu vermeiden und vorherzusehen, Dateien wiederherzustellen aber auch Bedrohungsszenarien zu simulieren und daraus allfällige Schulungen zu entwickeln. Außerdem werden Benchmarks im Vergleich zum Sicherheitsrisiko anderer Firmen erstellt, forensische Berichte geliefert sowie Empfehlungen zur besseren Sicherheit geschaffen.

Zugriffsmöglichkeiten werden mit einer Sicherheitsstufe versehen, die aus mehreren eindeutigen und/oder einmaligen Identifizierungsmerkmalen besteht (z. B. PIN, TAN und Passwort = 3-Faktor-Authentifizierung). Ein sicheres Identitätsmanagement ist für das Arbeiten in der Cloud unbedingt erforderlich, damit Zugriffe von Unbefugten (z. B. von Unternehmensexternen) nicht passieren können. Das Programm zur Verschlüsselung von Festplatten mobiler Geräte heißt bei MS „bitlocker".
„Windows Hello" bietet biometrische Zugriffskontrolle an (z. B. Fingerprint, Iris-Scan), um eine eindeutige Authentifizierung zu ermöglichen. Biometrische Zugriffssperren werden vor allem beim Zugriff zu Cloud-Services von MS genutzt, um Nutzer:innen automatisch informieren zu können, sollten ihre Passwörter/PINs im Dark Web verkauft werden.

Administrator:innen können in der „MS Security and Compliance Suite" einrichten, dass personenbezogene Daten wie IP-Adressen, Betreffzeilen oder gar Inhalte nicht an MS übermittelt werden.

In einer BV sollte auf folgendes geachtet werden:

- Zweck festlegen (z. B. Auswertung und Korrektur von Fehlern)
- 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)
- 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 einen hochsicherheitsrelevanten Nutzer:innenkreis zulassen

AZURE ACTIVE DIRECTORY

Auf Azure werden sämtliche Dateien und Vorgänge gespeichert. Azure stellt quasi den Konkurrenten zum Amazon-Speicheruniversum dar, dessen Kapazitäten MS aber (noch) nicht erreicht hat.

Das Active Directory ist sozusagen der „Türsteher" für sämtliche Anwendungen. „Einmal hin, alles drin." er-

klärt es flott ein Systemadministrator. Im Active Directory melden sich die Nutzer:innen an und identifizieren sich, wobei die IP-Adresse ebenso automatisch gespeichert wird, wie der Standort – so diese Funktion freigegeben wurde. Im AD wird bestimmt wer, wozu Zugriff hat. Es wird der Zugriff sämtlicher Geräte und Anwendungen reguliert. Im Azure Active Directory (AD) kann das bestehende App-Angebot erweitert werden. Azure ist die Plattform von MS auf der alle Apps für alle Nutzer:innen zur Verfügung gestellt werden.
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 zu den Apps unterschiedlich sicher.

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 Zustimmung ebenso unzulässig sind (DSB Entscheidung D124.2941). Umso überschießender wird es sein, ein solch heikles Merkmal für Vorgänge wie das Einloggen in Outlook zu verwenden.
Die Anmeldevorgänge werden aufgezeichnet und somit haben Administrator:innen die Möglichkeit gewisse Verhaltensmuster abzuleiten (z. B. Wer meldet sich wann in welcher App an? Von welchem Standort melden sich der/die Nutzer:in an? Für welche Dienste meldet sich wer besonders häufig an? Gibt es ein auffälliges Verhalten hinsichtlich der Anmeldezeitpunkte?).
Derzeit stehen über Azure etwa 130 Services zur Verfügung.

Zu regeln ist:

- Berechtigungskonzept (Möglichkeit für einfache Nutzer:innen, weitere Apps aus dem Katalog hinzuzufügen eher unterbinden)

- Für den Zugang zu besonders schützenswerten Daten eine 3-Faktor- Authentifizierung verwenden

- Berichte lesende Rolle für den BR vereinbaren

- Eindeutige Zwecke, wofür Azure verwendet werden darf

- Verhaltensauswertung nur ohne personenbezogene Vergleiche

- Löschfristen für Überwachungsprotokolle festlegen

- Allfällige Verwendung privater Geräte und deren Zugang regeln

- Grundsätzlich keine biometrische Identifikation ODER biometrische Authentifizierung nur auf freiwilliger Basis, verschlüsselt und ohne Zugang für betriebliche Administrator:innen ODER: biometrische Authentifizierung via „Windows Hello" ausschließlich für einen hochsicherheitsrelevanten Nutzer:innenkreis zulassen

AZURE INFORMATION PROTECTION

Sämtliche Informationen werden in der Azure Information Protection (AIP) klassifiziert, um das Schutzniveau zu bestimmen.

- niedriger Schutz = „public"
- normaler Schutz = „general"
- höchster Schutz = „highly confidential"

Kreditkarteninformationen, Geschäftsgeheimnisse werden wohl dem höchsten Schutzniveau zugeteilt und ihre Zugriffe, allfällige Weitergabe etc. genauestens nachvollzogen. Es könnte dadurch herausgefunden werden, ob strafrechtlich relevante Ereignisse stattgefunden haben (z. B. Betrug, Spionage, Insider-Handel, aber auch harmlosere Compliance-Verstöße wie solche gegen Kleidervorschriften). Eine anlasslose flächendeckende Durchleuchtung aller Dokumente, die vornehmlich dem Schutz vor falscher Verwendung dient, kann jedoch problematisch werden (z. B. BR-Korrespondenz, sämtliche E-Mails der Belegschaft des letzten halben Jahres etc.).

MS bietet auch AIP an, die „selbständig lernen", wie Daten zu klassifizieren sind. Das kann erst recht Probleme verursachen, wenn Korrespondenz auf Diffamierungen hin durchsucht wird.

Eine Einteilung zu Schutzniveaus sollte entlang der Zwecke vorgenommen werden, denen die Daten dienen. Nutzen bringt eine solche Klassifizierung indem für jede Klassifikationsstufe eindeutig festgelegt wird, wer Zugriff auf die Daten hat.

Dazu ein grobes Raster:

- Stammdaten der Beschäftigten → für HR und allenfalls Vorgesetzte
- Funktionsdaten, die aufgrund der Programmierung/ Einstellung der Anwendungen entstehen → für IT
- Inhaltsdaten, die durch das Arbeiten in den Anwendungen entstehen → für Beschäftigtengruppen je nach ihrer Arbeitsaufgabe
- diagnostische Daten, Protokoll-, Verkehrs- und Telemetriedaten, die im Hintergrund anfallen → diese Datenarten sollten möglichst deaktiviert sein bzw. rein für die Behebung technischer Gebrechen verwendet werden

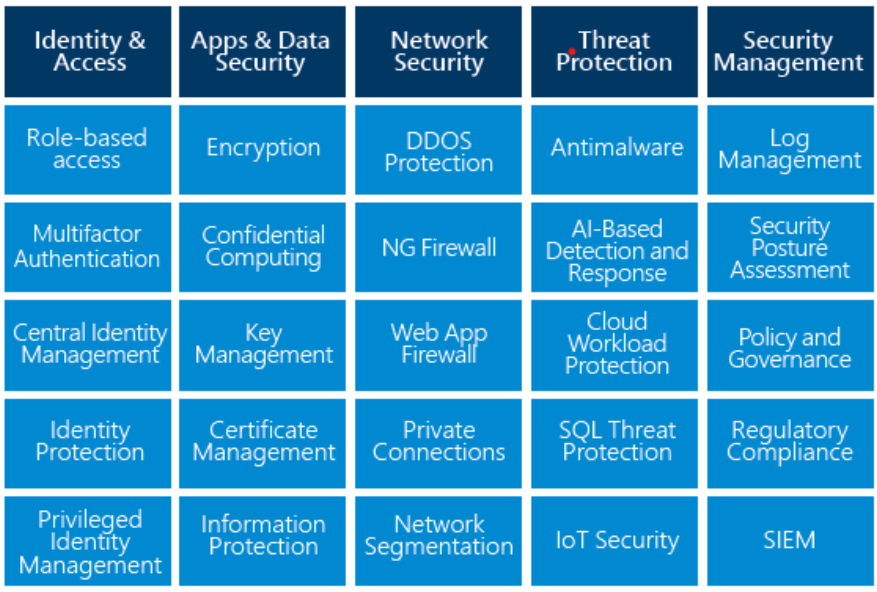
Eine (Risiko-)Klassifizierung ist erforderlich, um beim Verlust von Daten oder dem unberechtigten Zugriff auf Daten feststellen zu können, wie groß der entstandene Schaden für das Unternehmen oder eine Person ist. Keinesfalls sollte die Interpretation der Dateien, die im Zuge einer Analyse gefunden wurden, ohne Betriebsrat und ohne zur Verschwiegenheit verpflichteten Fachexpert:innen durchgeführt werden.

Azure Information Protection dient dazu, Informationen aus dem Betrieb zu schützen, auch wenn sie für die Zusammenarbeit mit betriebsexternen Personen verwendet werden. Mit der App kann nachverfolgt werden, welche Aktivitäten bei welchen Dateien vorgenommen werden.

In einer Betriebsvereinbarung sollte geregelt sein:

- Strenge Zugriffsregelungen
- Zweckbeschränkung auf juristische Belange und Angriffe auf die IT-Sicherheit
- Datenklassifikation je nach Vertraulichkeit mit Hilfe des Betriebsrats (eher keine rein automatisierte Klassifikation)
- Festlegen wie ein „gefährliches Ereignis“ definiert wird
- Klares Prozedere, was im Falle eines entdeckten „Risikos“ bzw. eines Verdachts zu geschehen hat (z. B. Zugriff sperren, Freigabe blockieren ...)
- Klare Speicherfristen für festgestellte „Ereignisse“

SAFETY- & SECURITY-APPS VON MS 365



SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

MS 365 bietet eine ganze Reihe Apps zur Sicherheit. Die verschiedenen Apps schützen vor unerlaubtem Eindringen, Entwenden von Daten, Einschleusen von Viren, Würmern und anderen unerwünschten Erscheinungen, zusammengefasst unter „safety & security" (z. B. Defender, SIEM – auf der Grafik rechts unten ist nur eine Möglichkeit der Gefahrenabwehr von vielen). Bei SIEM handelt sich um eine Sicherheits-App zur Auswertung und Prognose.

Durch die Analyse typischer Muster von Sicherheitsvorfällen, soll herausgefunden werden, ob ähnliche Vorfälle bevorstehen. In Echtzeit sollen Auffälligkeiten im Betriebssystem, in Datenbanken, in Apps analysiert und allfällige Sicherheitslücken behoben werden.

In einer Betriebsvereinbarung zu regeln:

- Zugriff auf die IT-Abteilung beschränkt
- Prozedere, was im Falle eines Verdachts oder bei tatsächlichen Sicherheitslücken zu geschehen hat
- um einer überschießenden Auswertung der Profile entgegenzuwirken, die „stufenweise Kontrollverdichtung" empfohlen (siehe Rahmen-Datenschutz-BV der GPA).

DATA LOSS PREVENTION (DLP)

Diese Anwendung zählt zu den Sicherheitsapps und dient, wie schon der Name ankündigt, dem Auffinden verloren gegangener Daten. Die Einstellungen dazu finden sich in „MS Purview Compliance Manager" [S. 66]. Hier kann festgestellt werden, ob Daten (illegal) abgegriffen wurden. Die Vorgaben, was als auffällige oder gefährliche Aktivität gilt, kann über Data Loss Prevention erstellt werden (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 schon nach vier Jahren statt wie vorgeschrieben nach sieben Jahren gelöscht werden).

Warnungen dürfen allerdings nicht die Arbeit des Betriebsrats beschränken. Wenn beispielsweise alle als „vertraulich" gekennzeichnete Dokumente mit Warnungen versehen werden, würde vieles was die Betriebsratsarbeit betrifft, behindert werden.

Die Regelungen sollen jenen in anderen Sicherheitsanwendungen von MS entsprechen (z. B. windows Hello, Threat Explorer, Bitlocker ...). Folglich sind auch hier die wichtigsten Punkte

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 geschehen hat
- Regeln für „Keywords" mit dem BR gemeinsam erstellen, um die Prüfung im Sinne der Interessenvertretung zu gestalten und übermäßige Überwachung (vertraulicher) Kommunikation hintanzuhalten
- Speicherfristen für festgestellte „Ereignisse"

INTUNE

Diese App ist dazu da, alle in einem Unternehmen registrierten mobilen Geräte zu verwalten und zu überprüfen. Intune scannt die vorhandenen mobilen Geräte beispielsweise auf Viren, ermöglicht den Fernzugriff und kann die Sperre von Accounts veranlassen. Über Intune können Geräte geortet werden. Die App dient dem Schutz der betrieblichen mobilen Infrastruktur, auch unter dem Namen „Mobile Device Management" (MDM) bekannt.

In einer BV regeln:

- Zugriffsmöglichkeiten auf IT-Abteilung beschränken
- 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

© iStock

NACHWORT

Bevor diese Broschüre gedruckt vorliegt, wird es zu einzelnen Passagen schon Neuigkeiten geben.

Der neuste Coup aus dem November 2022 ist eine gratis im Netz verfügbare „Künstliche Intelligenz", entwickelt in einem US-amerikanischen Unternehmen namens „OpenAI", dessen Leitung von der Gründung 2015 bis zu seinem Ausstieg 2018 der (derzeit) reichste Mann der Welt innehatte (Elon Musk), 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. Dieser ChatGPT (Chat Generative Pre-Trained Transformer) erfasst im Netz verfügbare Informationen und stellt sie zu, für viele überraschend hochwertigen, ethisch trainierten, eigenständigen Texten, Gedichten, Geschichten oder Bildern zusammen. Egal ob Hausübung, Zeitungsartikel, ein Bild im Van-Gogh-Stil, ein Drehbuch, ein Programmcode, ein Urlaubsreiseführer, eine Fehlersuche u.s.w., der Chatbot erfreut sich bei experimentierfreudigen Schüler:innen, IT-Aficionados, interessierten Studierenden, und vielen anderen großer Beliebtheit. ChatGPT ist MS den großzügigen Betrag von einer Milliarde Euro wert. Die Beteiligung soll demnächst um ein „zusätzliches milliardenschweres Investment bei OpenAI" erweitert werden (wie der Standard am 23. Jänner 2023 berichtete). Mittels ChatGPT wird derzeit in der Welt von MS die Suchmaschine Bing leistungsfähiger, Konferenzen besser zusammengefasst, die Übersetzung auf Teams-Konferenzen von Ton in Text optimiert etc. ChatGPT soll in einer Version „Prometheus" von MS weiterentwickelt, durch Quellenangaben ergänzt und so, auch wissenschaftlich gesehen, attraktiver werden (wie der Standard am 7.2.2023 berichtete). Momentan steigt vor allem der Wert von Microsoft-Aktien.

Die Prognose ist wenig gewagt, 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, die für permanente Veränderung und so manche Überraschungen sorgen, werden rechtlichen Rahmenbedingungen und die generelle, breit aufgestellte Ausrichtung von MS gleichbleiben – so wie auch die Pflicht, zu MS 365 eine Betriebsvereinbarung zu vereinbaren. Dieser Text soll dabei helfen, den Überblick zu bewahren und die beste zum Unternehmen passende Betriebsvereinbarung auszuhandeln.

CHECKLISTE: WAS IN EINER (BASIS-)BETRIEBSVEREINBARUNG ZU MS 365 ZU REGELN IST

- ☐ **Rechtsgrundlage** §§ 96 und 96a ArbVG (ev. in Verbindung mit Artikel 88 DSGVO)
- ☐ **Überblick** über aktivierte, im Betrieb verwendete Apps/Anwendungen von MS 365 (Checkliste [S. 73])
- ☐ 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. 21]
- ☐ **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. 33])
- ☐ **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. 55]) 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. Delve [S. 47] und Viva Insight [S. 50])
- ☐ **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
- ☐ Heimliche/verdeckte Aktionen unterbinden
- ☐ Erstellen von **Profilen** zur Leistungsbeurteilung unterbinden (z. B. Ranking, Boni etc.)
- ☐ Umgang mit **Updates** regeln (Testläufe, Testuser:innen)
- ☐ Regelmäßige **Evaluierung** (vgl. § 4 ASchG [S. 22])

CHECKLISTE: IST MS 365 IN EINKLANG MIT DER 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, Empfängerkreise, Verantwortliche, 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?

CHECKLISTE DER MS 365 APPS

(für Lizenz E3 mit Release Jänner 2023)

Anwendung/ Komponente	ja/nein/geplant	Verwendungszweck/ Funktion	Betriebsver-einbarung ja/ nein/in Arbeit	Anmerkungen
3rd Party Integration for MFA [1]				
Activity Reports[2]				
Administrative Units[3]				
Adoption Score[4]				
AI Builder[5]				
Alert Policies[6]				
App Proxy including PingAccess[7]				
Application Control & Application Guard[8]				
App Locker[9]				
Audit (standard)[10]				
Automated Investigation & Response[11]				
Azure AD[12]				
Azure AD Connect Health[13]				
BitLocker[14]				
Block at First Sight[15]				
Bookings[16]				
Briefing Email[17]				
Cloud App Discovery[18]				
Compliance Manager[19]				
Conditional Access[20]				
Cortana[21]				
Cross-Plattform Support[22]				
Data Loss Prevention[23]				
Dataverse[24]				
Defender Antivirus[25]				
Defender EASM[26]				
Dynamic Groups[27]				
Dynamics 365[28]				
Dynamics 365 Customer Voice[29]				
Edge[30]				
EHR Connector for Teams[31]				
Endpoints Analytics, Detection & Response[32]				
Enhanced ASR[33]				
Enterprise State Roaming[34]				
Exchange Online Archiving[35]				
External Identities[36]				
Forms[37]				
Graph Connector[38]				
Identity Manager[39]				
Information Protection[40]				

Anwendung/ Komponente	ja/nein/geplant	Verwendungszweck/ Funktion	Betriebsver-einbarung ja/ nein/in Arbeit	Anmerkungen
Insights by MyAnalytics[41]				
Intune[42]				
Lists[43]				
Litigation Hold & eDiscovery[44]				
Mobile Device Management (MDM)[45]				
Message Encryption[46]				
Mobility & Security[47]				
Multi-Factor Auth (MFA)[48]				
OneDrive[49]				
Password Protection[50]				
Planner[51]				
Power Apps[52]				
Power Automate[53]				
Power Virtual Agents[54]				
Project & Roadmap View Access[55]				
Purview[56]				
Search[57]				
Secure Score[58]				
Self-Service Group Management[59]				
Self-Service Password Reset[60]				
Sentinel[61]				
Single-Sign- On[62]				
Stream[63]				
Sway[64]				
Syntex[65]				
Teams[66]				
Teams Rooms[67]				
Temporary Acess Pass[68]				
Threat Analystics[69]				
To Do[70]				
Viva Connections[71]				
Viva Engage[72]				
Viva Goals[73]				
Viva Insights[74]				
Viva Learning[75]				
Viva Sales[76]				
Viva Suite[77]				
Viva Topics[78]				
Vulnerability Management[79]				
Webinars[80]				
Whiteboard[81]				
Windows Firewall[82]				
Windows Hello[83]				
Yammer Enterprise[84]				

[1] Über die App *3rd-Partie-MFA-Integration* können Multifaktor-Authentifizierungen verwendet werden (d.h. Login mit mehreren, die Identität bestätigenden Faktoren, meist bestehend aus Passwort, SMS-Code plus Benutzername), wobei Drittfirmen einen oder mehrere der Faktoren beisteuern.
[2] *Activity Reports* (deutsch: Nutzungsberichte) werden im Admin-Center zu sämtlichen MS 365-Apps mit sämtlichen gewünschten Komponenten zur Verfügung gestellt (z. B. E-Mail-Nutzungshäufigkeit der letzten 30 Tage auf dem *Exchange* Server).
[3] Die *Administrative Units* sind beliebige Abschnitte im Azure Verwaltungsbereich, die für Admins bereitgestellt werden. Sie definieren deren Zuständigkeit z. B. für eine Region, einen Logistikbereich.
[4] Der *Adoption Score* (deutsch etwa: Anpassungswert) vergibt eine Punktwertung, wie weit fortgeschritten ein Betrieb in der „Digitalisierung" ist, wofür MS365-Daten über Kollaboration, Mobilität, Kommunikation, Meetings etc. verwendet. Heraus kommen Optimierungsvorschläge wie etwa: „Menschen, die in der Cloud zusammenarbeiten und Inhalte teilen, anstatt Anhänge per E-Mail zu versenden, können bis zu 100 Minuten pro Woche einsparen." Alle Erkenntnisse werden anhand von Daten auf Organisationsebene berechnet, nicht auf individueller Ebene.
[5] Der *AI Builder* (deutsch etwa: Erbauer Künstlicher Intelligenz) ist eine Funktion aus den *Related Services* (deutsch etwa: erweiterten Leistungen) von MS 365, die mittels maschinellem Lernen Geschäftsprozesse „verbessert", ohne dass ausgefeilte Programmierkenntnisse erforderlich sind. Der *AI Builder* steht in Apps wie *Dynamics 365*, *Power Apps* und *Power Automate* zur Verfügung.
[6] *Alert Policies* (deutsch: Warnungsrichtlinien), werden entweder im *MS Purview-Compliance-Portal* oder im *MS 365 Defender-Portal* erstellt und warnen je nach den zugrunde gelegten Parametern vor Risiken.
[7] Die App *Proxy* (das ist ein Rechner als Schnittstelle zwischen verschiedenen Netzwerken) ermöglicht es Nutzer:innen ohne VPN-Tunnel in das Unternehmensnetzwerk bzw. MS 365 einzusteigen. *Proxy* ist Teil des *Azure Active Directory*.
[8] Die *Application Controll* und der *Application Guard* (deutsch etwa: Anwendungskontrolle und Anwendungs-Wächter) sind Sicherheitstools im Betriebssystem *Windows*. Die hier erstellten Richtlinien können verhindern, dass Schadsoftware auf den Apps landet und bestimmt, welche Skripts (Befehlketten innerhalb von Programmen) durchgeführt werden dürfen.
[9] Der App Locker im Betriebssystem Windows definiert, welche Anwendungen, Hersteller, Programme, Dateipfade oder auch Skripts (Befehlketten innerhalb von Programmen) ausgeführt werden dürfen.
[10] *Audit* gehört zu Security-and-Compliance-Apps von *MS Purview*. *Audit* schreibt die Protokolle sämtlicher Apps und kann nach sämtlichen Ereignissen suchen und diese bei Bedarf importieren.
[11] Die *Automatisierte Untersuchung und Reaktion* ist eine App im *MS Defender*. Damit soll es den Administrator:innen erleichtert werden auf Alarme zu reagieren indem die Alarme nach Wichtigkeit klassifiziert werden und standardmäßig Richtlinien hinterlegt werden.
[12] *Azure Active Directory* ist die Verwaltungszentrale von MS 365, die für (Multi-Faktor-)Authentifizierung, Zugriffs- und Berechtigungssteuerung zuständig ist.
[13] Die Bezeichnung *Health* bezieht sich auf die Gesundheit der IT, nicht der Nutzer:innen. Connect Health überwacht ob sich die richtigen Nutzer:innen zum richtigen Zeitpunkt in die richtigen Apps mit den richtigen Authentifizierungen angemeldet haben.
[14] *BitLocker* ist die Verschlüsselungsfunktion des MS Betriebssystems *Windows*. Dateien auf Exchange Online, SharePoint Online und Skype for Business werden damit vor fremdem Zugriff geschützt.
[15] *„Auf den ersten Blick sperren"* ist Teil des *MS Defender* und verwendet maschinelles Lernen und automatisiertes Analysieren, um festzustellen, ob Dateien eine Bedrohung enthalten.
[16] *Booking* ist eine App zur Terminkoordination (ebenso wie der *Outlook*-Kalender oder *Teams* oder *Planner*, mit denen *Booking* auch verlinkt) ergänzt um Terminkoordination mit Kund:innen, Klient:innen, Geschäftspartner:innen etc. und deren Vorlieben.
[17] Die App *Briefing E-Mail* fasst die „relevanten" Ereignisse des Tages auf Basis von E-Mails zusammen inklusive der dafür „erforderlichen" Dokumente, „wichtigen" Personen oder empfohlener Fokuszeiten.
[18] Die *Cloud App Discovery* ist Teil des *MS Defenders* und überwacht sämtliche MS 365-Infrastruktur, die in der Cloud liegt.
[19] Die App *Compliance Manager* aus dem *MS Purview-Portal* hilft beim Abschätzen von Datenschutzrisiken, bei Kontrollen, beim Einhalten von Vorschriften und Zertifizierungen und bei den Berichten für Prüfer:innen.
[20] Die App *Conditional Access* (bedingter Zugriff) steuert im *Azure AD* die Richtlinien, wer individuell, wann genau, worauf Zugriff hat.
[21] *Cortana* ist die Sprachassistentin von MS 365, man könnte auch sagen, die etwas weniger bekannte „kleine Schwester" von Alexa/Siri.
[22] Mit *Cross-Platform Support* (deutsch etwa: Plattform übergreifende Unterstützung) können weitere Apps eingebunden oder deren Features in MS *Teams* erstellt werden, ohne dass die Nutzer:innen bei der Verwendung dieser externen Programme Teams verlassen.
[23] Die App *Data Loss Prevention* ist Teil des *MS Purview*, damit also ein Sicherheits- und Security-Tool. Damit werden Richtlinien definiert, wie vertrauliche Dateien besser geschützt werden (z. B. Suche nach Schlüsselwörtern, auffälligen Dateimengen, besonderen Empfängerkreisen u.s.w.). Algorithmen, die selbsttätig Auffälligkeiten erkennen sollen, sind Teil der App.
[24] Das *Dataverse* ist der Platz an dem alles gespeichert und verwaltet wird. Sämtliche Telemetrie- und Nutzer:innen:daten kommen aus diesem „Datenuniversum".
[25] Der *Defender Antivirus* (vormals *„Windows Anti Spy"*) ist das Virenschutzprogramm der MS Betriebssysteme *Windows* 10 und 11.
[26] Die App *Microsoft Defender EASM (External Attack Surface Management)* dient dem vorausschauenden Sicherheitsmanagement. Es umfasst (noch unbekannte) Bedrohungsszenarien, die außerhalb der klassischen Firewall liegen. Für die MS 365 Umgebung arbeitet der *Defender* mit selbstlernenden Algorithmen.
[27] Mit der App *Dynamic Groups* können im *Azure AD* Berechtigungen so vergeben werden, dass die jeweilige Gruppenzugehörigkeit variiert (z. B. je nach Gerät über das zugegriffen wird).
[28] *MS Dynamics* ist ein eigenes Programm zur Personalverwaltung. Es beinhaltet u.a. Zeiterfassung, Qualifikationen, Lohnverrechnung, Urlaubsplanung, On- und Off-Boarding, Berichtswesen, u.s.w. *Dynamics* ist ein eigenständiges Programmpaket aus dem Hause MS, das (derzeit) nicht in MS 365 integriert ist, aber eingehängt werden kann.
[29] *Dynamics 365 Customer Voice* (deutsch: Stimme der Kund:innen) ist eine Erweiterung (related service), die umfangreiche Funktionen im Bereich des Kundenmanagements (CRM) anbietet (z. B. Termine, Umfragen, Zufriedenheit, Stimmung, Empfehlungen, Prognosen), wofür auch Algorithmen eingesetzt werden, die mittels vorhandenem Datenmaterial Prognosen erstellen.
[30] *Edge* ist der Browser von MS. Ein Browser „stöbert" im Internet, stellt die Webseiten dar. (Der frühere MS Browser Explorer wurde mit Juni 2022 für das Betriebssystem Windows 10 nicht mehr bereitgestellt.)
[31] Der *Microsoft Teams Electronic Health Record (EHR) Connector* liefert den zugriffsberechtigten Admins eine detaillierte Übersicht zur *Teams*-Nutzung (z. B. Lizenzüberschreitungen, Daten, Mitglieder, Files, Dauer u.s.w.).
[32] Mit der App *Endpoint Analytics* werden sämtliche Geräte überprüft und Administrator:innen auf allfällige Schwachstellen hingewiesen. Die Analyse erfolgt über die Geräteverwaltung *Intune*.
[33] *Enhanced Attack surface reduction (ASR)* sind Teil des *MS Defender*, also zur Sicherheit gedacht. In der App können speziell auf das Unternehmen abgestimmte Sicherheitsrichtlinien erstellt werden, die potentielle Angriffsflächen reduzieren (z. B. Download verhindern, verdächtige Skripts blocken und Ähnliches).
[34] *Enterprise State Roaming* liegt im Verwaltungszentrum *Azure AD* und sucht den für das Unternehmen passenden Standort für Datenverarbeitung, das Hosting auf den MS Servern.
[35] *Exchange Online Archiving* speichert und archiviert sämtliche Daten des *Exchange-Servers*, wenn dieser in der Cloud verwendet wird.
[36] Mit der App *External Identities* können im *Azure AD* Nutzer:innen eingebunden werden, die außerhalb des Unternehmens angesiedelt sind (z. B. Klient:innen, Lieferant:innen, Kund:innen, Geschäftspartner:innen).
[37] *Forms* ist eine Software zur Erstellung von Umfragen.
[38] Mit der App *Graph Connector* können aus dem alles mitprotokollierenden Graph Verbindungen – wohin auch immer man möchte – hergestellt werden, z. B. für Auswertungen oder Suchen. Es handelt sich um eine Erweiterung von MS 365 (related Service; deutsch etwa: verwandte Dienstleistung).
[39] Mit dem *Identity Management* werden in *Azure AD* die Zugriffsberechtigungen verwaltet und können über *Azure* hinausgehend – etwa mit unternehmenseigenen Systemen – verknüpft werden (z. B. Personalverwaltung aus SAP).
[40] Die App I*nformation Protection im MS Purview Portal* soll Dateien klassifizieren und entsprechend schützen. Dazu wird ein selbstlernender Algorithmus eingesetzt.

[41] *Analytics* stellt persönliche Auswertungen zum Nutzungsverhalten zusammen. Es ist nicht ratsam, *Analytics* zu aktivieren. Falls es sein muss, sollte es ausschließlich den Betroffenen selbst zur Verfügung stehen. Die Empfehlungen von *Analytics* sind keinesfalls als Arbeitsvorgaben oder Leistungsbewertungen zu interpretieren.
[42] Auf *Intune* werden mobile Geräte und auf ihnen befindliche Apps verwaltet.
[43] Die App *Lists* soll Prozesse, Projekte, Aufgaben strukturieren. Sie fasst beliebige Inhalte (z. B. Termine, Themen, Dokumente) für beliebige Personen (z. B. Einzelne, Abteilungen, Gruppen) in beliebigem Format (z. B. Tabelle, Kalender) zusammen und unterstütz auch mit Vorschlägen eines selbstlernenden Algorithmus.
[44] *Litigation Hold* und *E-Discovery* sind Teile des *MS Purview Compliance Centers*. Mit der App werden eigene Aufbewahrungs-Rrichtlinien für Beweissicherungsverfahren und Beweissuche erstellt. Auch gelöschte, archivierte oder verlorene Dateien können wieder hergestellt werden.
[45] Das *Mobile Device Management (MDM)* erfolgt in der App Intune und verwaltet sämtliche Geräte des *M 365 Universums*, inklusive Sensoren, Maschinen, Drucker, Handys u.s.w.
[46] Die App *Message Encryption* ermöglichet verschlüsselte Kommunikation innerh alb und außerhalb eines Unternehmens. Sie ist Teil des *MS Purview Compliance Centers*.
[47] Bei *Mobility & Security* wird die Sicherheit für mobile Geräte und deren Apps verwaltet.
[48] Mit der App können *Multifaktor-Authentifizierungen*, also das LogIn über mehrere, die Identität bestätigende Faktoren, i.d.R. Passwort, Code per SMS plus Benutzername, gesteuert werden
[49] *OneDrive* dient dem Organisieren von Texten, Notizen, Bildern etc. und ist als individuelle Ablage gedacht. Dateien können aber auch für andere freigegeben werden.
[50] Die App *Password Protection* (deutsch: Passwortschutz) dient der Organisation von Passwörtern, enthält gesperrte Listen, wie ein Passwort nicht aussehen darf und kann betriebsspezifisch erweitert werden. Sie ist Teil des „Verwaltungszentrums" *Azure AD*.
[51] Der *Planner* ist eine App mit der (gemeinsam) Projekte geplant, Aufgaben verteilt, Deadlines gesetzt werden können.
[52] Mit *Power Apps* können auch Nicht-Programmierer:innen Apps erstellen.
[53] Mit *Power Automate* können eigene automatisierte Abläufe kreiert werden bzw. Apps nach persönlichen Wünschen, zusätzlich zu den bestehenden, zusammengestellt werden.
[54] Der *Power Virtual Agent* ist der *ChatBot* von MS, also ein Programm das, automatisiert und selbstlernend auf Fragen von Nutzer:innen Antworten schreibt
(z. B. auf *Teams*). Er kann relativ einfach programmiert werden.
[55] *Project* ist ein umfangreiches Tool zur Planung, Steuerung und Überwachung von Projekten. Die App enthält Qualifikationen, Multiprojektmanagement, Zeiterfassung, zentrale Ressourcenplanung, Risiko-, Dokumentenmanagement, Zugriffsverwaltung, Reporting etc.
[56] *MS Purview* ist die App mit der sämtliche Sicherheitsfunktionen gesteuert werden. *Purview* ist zuständig für den Überblick und die Risikobewertung, die Gefahrenabwehr und die *Compliance*, die Kommunikationsrichtlinien und die Löschfristen u.s.w.
[57] *Search* ist eine MS-interne Suchfunktion, die in (fast) allen Apps zur Verfügung steht und App-übergreifend sucht. Search basiert auf der MS Suchmaschine Bing und liefert Ergebnisse zu beliebigen App-internen Suchen (z. B. Personen, Dateien, Organigrammen, Websites etc.).
[58] Der *Secure Score* ist eine App innerhalb des *MS Defender*. Der *Secure Score* liefert Berichte über die Sicherheit des Unternehmens, sowie Vergleiche mit anderen Unternehmen und erstellt so Schwellenwerte (Benchmarks) aufgrund derer MS Verbesserungen für die *Safety & Security* empfiehlt.
[59] Die App *Self-Service Group* ist Teil des *Azure AD* und dient der (Selbst-) Organisation von Gruppen mit gleichen Berechtigungen, wo also die Mitglieder an denselben Prozessen teilhaben bzw. sie bearbeiten können sollen und selbst den Kreis der Mitglieder erweitern sollen.
[60] *Self-Service Password Reset* dient dazu, dassnn Nutzer:innen selbständig ihr Passwort zurücksetzen können.
[61] Die App *Sentinel* (zu deutschzu Deutsch: Wächter) registriert sicherheitsrelevante Vorfälle, auch solche, die außerhalb des MS Universums, beispielsweise in verlinkten Apps stattfinden. Sie korrespondiert in der Regel über das *Azure AD* mit dem *MS Defender* und erweitert so die aufgezeichneten sicherheitsgefährdenden Ereignisse.
[62] Die App *Single-Sign-On to other SaaS* ist Teil der *Enterprise Mobility & Security Suite* von MS 365 und ermöglicht es den Nutzer:innen mit einem einzigen Passwort in sämtliche Apps, auch außerhalb des MS 365 Universums, einzusteigen.
[63] Auf der App *Stream* können Nutzer:innen selbst hergestellte Videos hochladen, ansehen, kommentieren, bewerten. Stream funktioniert ähnliche einem unternehmensinternen *YouTube*-Kanal.
[64] *Sway* ist eine Software für Präsentationen. Die Daten werden in den USA gespeichert.
[65] *Syntex* ist eine App, die MS unter der Überschrift *„Automation & Intelligence"* als Ergänzung anbietet. Syntex macht mittels „Künstlicher Intelligenz" Übersetzungen, Zusammenfassungen, Anmerkungen etc. (z. B. in Teams).
[66] *Teams* ist eine App mit umfassenden Möglichkeiten zur Kommunikation und Kollaboration.
[67] Über die App Teams *Rooms* können innerhalb eines Video-Calls auf *Teams* kleinere (Arbeits-)Gruppen gebildet werden, um mehr „Privatsphäre" zu ermöglichen.
[68] Über dem *Temporary Access Pass* (zu deutschzu Deutsch: temporärer Zutritt) können Nutzer:innen im *Enterprise Mobility & Security (EMS)* ohne eigenes Passwort für einzelne Apps für einen limitierten Zeitraum freigeschalten werden.
[69] *Threat Analytics* ist ein Teil von *MS Defender*. Damit werden sämtliche Apps gefiltert, um Sicherheitsgefahren abzuwenden. Es können eigene Projekte (sog. „Kampagnen") erstellt werden (z. B. gegen Phishing).
[70] *To Do* hieß vor dem Kauf durch MS „Wunderlist" und ist eine App um Aufgaben aus anderen Programmen (z. B. *Outlook*, *Planner*) zu einem eigenen, nur individuell einsehbaren (Tages-)Plan zusammenzustellen.
[71] Die App *Viva Connections* dient dazu, die wichtigsten Informationen unternehmensintern zu veröffentlichen, ist sozusagen das virtuelle „schwarze Brett".
[72] Die App *Viva Engage* dient dem persönlichen Austausch der Beschäftigten untereinander, ist sozusagen die „Ideenbörse" eines Unternehmens.
[73] Die App *Viva Goals* stellt die persönlichen Ziele von Beschäftigten dar und analysiert wie weit sie – im Vergleich mit anderen Beschäftigten – erreicht wurden.
[74] Die App *Viva Insights* bietet – basierend auf den bisherigen persönlichen Verhaltensdaten – Vorschläge zum effizienteren Arbeiten oder zum besseren Wohlbefinden (z. B. Pünktlichkeitsauswertungen, Fokuszeiten u.s.w.).
[75] Auf *Viva Learning* werden – abgestimmt auf das persönliche Verhalten – Lernprogramme vorgeschlagen (z. B. Skripten, Youtube-Tutorials), die entweder aus dem Unternehmen stammen oder von MS zusammengestellt sind.
[76] Die App *Viva Sales* dient dem Kundenbeziehungsmanagement-Tool (CRM) und empfiehlt – basierend auf den bestehenden Kontakten, Terminen, Kommunikationen und Social-Media-Aktivitäten und ergänzt um „künstliche Intelligenz" – welche Kundinnen und Kunden auf welche Art in welchem Zeitraum mit welchem Produkt angesprochen werden sollten.
[77] In der *Viva Suite* werden sämtliche anderen *Viva*-Apps im Überblick zusammengestellt und verwaltet.
[78] Mit der App *Viva Topics* soll unternehmensintern das Fachwissen von Expert:innen koordiniert werden. Themenkarten, Themenseiten und Themencenter sollen das unternehmensinterne Wissensmanagement – mit zusätzlicher Hilfe von selbstlernenden Algorithmen – erleichtern.
[79] Im *MS Vulnerability Management* kann untersucht werden, welche Auswirkungen allfällig neu erstellte Sicherheitsrichtlinien auf die gesamte MS 365 Infrastruktur erzielen können und welche Sicherheitsempfehlungen MS ableitet. Die App ist Teil des *MD Defender*.
[80] *Webinars* ist eine App im Rahmen der Kommunikationsplattform *Teams* für Veranstaltungen mit vielen Teilnehmenden.
[81] *Whiteboard* ist eine App auf der Usern und Userinnen die jeweils gewünschten Inhalte darstellen können (z. B. Grafiken, Tabellen, Schrift etc.), wobei diese Inhalte auch aus anderen MS 365-Apps übernommen werden können (z. B. *Powerpoint* aus *Office* oder *Sway*, während einer *Teams*-Sitzung).
[82] Die App *Windows Firewall* ist ein Sicherheitsfeature (also Teil des *MS Defenders*) des Betriebssystems *Windows*). Mit der Firewall werden Viren herausgefiltert, Schadsoftware abgewehrt und Ähnliches, sowie Berichte erstellt.
[83] *Windows Hello* ist eine App zur Authentifizierung mittels biometrischer Merkmale (z. B. Fingerabdruck, Gesicht), weshalb hier besondere Vorsicht gelten muss. Empfohlen werden kann das nur in streng limitierten Ausnahmefällen.
[84] Die App *Yammer Enterprise* ist ursprünglich ein unternehmensinterner Kurznachrichtendienst, der mittlerweile auch Kollaborations-Funktionen enthält (z. B. Dateien hochladen und bearbeiten).

WEITERFÜHRENDE UNTERLAGEN DER GEWERKSCHAFT GPA

Die Gewerkschaft GPA bietet eine große Sammlung an **Muster-BVen** und **Checklisten** zu einzelnen Systemen, die auch via MS 365 verwendet werden können. Diese werden von den betriebsbetreuenden KollegInnen gerne zur Verfügung gestellt – und bei Bedarf mit einer auf den Betrieb angepassten Beratung ergänzt.

- Muster-BV Telefonsysteme (Teams [S. 42])
- Muster-BV Dokumentenmanagement (OneDrive [S. 55], Delve [S. 47])
- Muster-BV Mobile Device Management (Intune [S. 69])
- Muster-BV Zutritt (Compliance Manager [S. 66])
- Leitfaden Mitarbeiterumfrage (Forms [S. 54])
- Muster-Module Videokonferenzsystem (Teams [S. 42])
- Checkliste Rankings (Viva [S. 50])
- Arbeitsunterlage Einsicht in E-Mails (z. B. für Outlook [S. 39], Teams [S. 42])
- Muster Rahmen-BV

Seibold, Bettina; Mugler, Walter (Böckler Stiftung): Dynamische Prozessvereinbarung für Cloud-Software wie Microsoft Office 365 (2022) Betriebs- und Dienstvereinbarungen, 15 Seiten
[als Download https://www.boeckler.de/de/faust-detail.htm?sync_id=HBS-008272]

BROSCHÜREN DER GEWERKSCHAFT GPA

Sozial? Digital? Mit Potenzial?
Personalentwicklung aus Sicht des Betriebsrats

Whistleblowing
Rechtliche Hintergründe und Tipps für die Praxis

Lost in Homeoffice?
Neue Rechtsgrundlage 2021 und aktuelle Gestaltungstipps

Die europäische Datenschutzgrundverordnung
aus ArbeitnehmerInnensicht

JA! ICH WERDE JETZT GPA-MITGLIED!

☐ Frau ☐ Herr ☐ Divers ☐ .....

Titel .....

Familienname.....

Vorname .....

Geburtsdatum

Straße/Hausnr. .....

PLZ/Wohnort.....

Telefonisch erreichbar .....

E-Mail.....

Damit wir dich bei Kollektivvertragsverhandlungen richtig informieren können, bitten wir um Angabe deines Dienstgebers und der genauen Branche.

Beschäftigt bei .....

Anschrift .....

Branche .....

Derzeitige Tätigkeit.....

Zutreffendes bitte ankreuzen:

☐ Angestellte:r ☐ Arbeiter:in ☐ Lehrling/..... Lj.

☐ Schüler:in ☐ Student:in ☐ Werkvertrag

☐ Zeitarbeitskraft ☐ freier Dienstvertrag

☐ Zweitmitgliedschaft ☐ geringfügig beschäftigt

GPA-Beitrittsmonat/-jahr: .....

Gehaltshöhe brutto .....

Der monatliche Mitgliedsbeitrag beträgt 1 % des Bruttogehalts bis zu einem Maximalbeitrag, der jährlich angepasst wird (siehe **www.gpa.at/mitgliedsbeitrag**). Der Mitgliedsbeitrag ist steuerlich absetzbar.

☐ Ich willige ein, dass ÖGB, ÖGB Verlag und/oder VÖGB mich telefonisch bzw. per elektronischer Post (§107 TKG) kontaktieren dürfen, um über Serviceleistungen, etwa Aktionen für Tickets, Bücher und Veranstaltungen zu informieren und sonstige Informationen zu übermitteln. Die Einwilligung kann jederzeit widerrufen werden.

Ich bezahle meinen Mitgliedsbeitrag durch: (Zutreffendes bitte ankreuzen)

☐ **Betriebsabzug**

Ich erkläre, dass mein Gewerkschaftsbeitrag durch meinen Arbeitgeber von meinem Gehalt/Lohn/Lehrlingseinkommen abgezogen werden kann. Ich erteile deshalb meine Einwilligung, dass meine im Zusammenhang mit der Beitragseinhebung erforderlichen personenbezogenen Daten (angegebene Daten und Gewerkschaftszugehörigkeit, Beitragsdaten, KV-Zugehörigkeit, Eintritts-/und Austrittsdaten, Karenzzeiten, Präsenz-, Ausbildungs- und Zivildienstzeiten, Pensionierung und Adressänderungen) von meinem Arbeitgeber und von der Gewerkschaft verarbeitet werden dürfen, wobei ich diese Einwilligung zum Betriebsabzug jederzeit widerrufen kann.

☐ **SEPA Lastschrift-Mandat** (Bankeinzug)

Ich ermächtige die Gewerkschaft GPA, die Zahlungen meines Mitgliedsbeitrages von meinem Konto mittels SEPA-Lastschrift einzuziehen. Zugleich weise ich mein Kreditinstitut an, die von der Gewerkschaft GPA auf mein Konto gezogene SEPA-Lastschriften einzulösen. Ich kann innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrags verlangen. Es gelten dabei die mit meinem Kreditinstitut vereinbarten Bedingungen.

Der Einzug des Mitgliedsbeitrages erfolgt jeweils zum Monatsultimo.

Wenn ich dem Betriebsabzug zugestimmt habe, diesen aber nicht mehr wünsche oder aus dem Betrieb ausscheide oder der Abzug des Mitgliedsbeitrages über den Betrieb nicht mehr möglich ist, ersuche ich die Zahlungsart ohne Rücksprache auf SEPA-Lastschrift von meinem bekannt gegebenen Konto umzustellen.

IBAN

BIC

.....
Datum/Unterschrift

Ich bestätige, nachstehende Datenschutzerklärung (auch abrufbar unter www.oegb.at/datenschutz) zur Kenntnis genommen zu haben.

.....
Datum/Unterschrift

ÖGB-ZVR-Nr.: 576439352, CID: AT48ZZZ00000006541

DATENSCHUTZINFORMATION (online unter: **www.oegb.at/datenschutz**)

Der Schutz Ihrer persönlichen Daten ist uns ein besonderes Anliegen. In dieser Datenschutzinformation informieren wir Sie über die wichtigsten Aspekte der Datenverarbeitung im Rahmen der Mitgliederverwaltung. Eine umfassende Information, wie der ÖGB/die Gewerkschaft GPA, mit Ihren personenbezogenen Daten umgeht, finden Sie unter www.oegb.at/datenschutz.

Verantwortlicher für die Verarbeitung Ihrer Daten ist der Österreichische Gewerkschaftsbund. Wir verarbeiten die von Ihnen angegebenen Daten mit hoher Vertraulichkeit, nur für Zwecke der Mitgliederverwaltung der Gewerkschaft und für die Dauer Ihrer Mitgliedschaft bzw. solange noch Ansprüche aus der Mitgliedschaft bestehen können. Rechtliche Basis der Datenverarbeitung ist Ihre Mitgliedschaft im ÖGB/in der Gewerkschaft GPA; soweit Sie dem Betriebsabzug zugestimmt haben, Ihre Einwilligung zur Verarbeitung der dafür zusätzlich erforderlichen Daten.

Die Datenverarbeitung erfolgt durch den ÖGB/die Gewerkschaft GPA selbst oder durch von diesem vertraglich beauftragte und kontrollierte Auftragsverarbeiter. Eine sonstige Weitergabe der Daten an Dritte erfolgt nicht oder nur mit Ihrer ausdrücklichen Zustimmung. Die Datenverarbeitung erfolgt ausschließlich im EU-Inland.

Ihnen stehen gegenüber dem ÖGB/der Gewerkschaft GPA in Bezug auf die Verarbeitung Ihrer personenbezogenen Daten die Rechte auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung zu. Gegen eine Ihrer Ansicht nach unzulässige Verarbeitung Ihrer Daten können Sie jederzeit eine Beschwerde an die österreichische Datenschutzbehörde (www.dsb.gv.at) als Aufsichtsstelle erheben.

Sie erreichen uns über folgende Kontaktdaten:

Gewerkschaft GPA
1030 Wien, Alfred-Dallinger-Platz 1
Tel.: +43 (0)5 0301
E-Mail: service@gpa.at

Österreichischer Gewerkschaftsbund
1020 Wien, Johann-Böhm-Platz 1
Tel.: +43 (0)1 534 44-0
E-Mail: oegb@oegb.at

Unseren Datenschutzbeauftragten erreichen Sie unter **datenschutzbeauftragter@oegb.at**.

Bitte die ausgefüllte Mitgliedsanmeldung beim Betriebsrat abgeben oder in ein frankiertes Kuvert stecken und senden an: **Gewerkschaft GPA,** Service Center, Alfred-Dallinger-Platz 1, 1030 Wien

GEWERKSCHAFT GPA
IN GANZ ÖSTERREICH

SERVICE-HOTLINE:
+43 (0)5 0301

GEWERKSCHAFT GPA
Service-Center
1030 Wien, Alfred-Dallinger-Platz 1
Tel.: +43 (0)5 0301
Fax: +43 (0)5 0301-300
E-Mail: service@gpa.at

GPA Wien
1030 Wien, Alfred-Dallinger-Platz 1

GPA Niederösterreich
3100 St. Pölten, Gewerkschaftsplatz 1

GPA Burgenland
7000 Eisenstadt, Wiener Straße 7

GPA Steiermark
8020 Graz, Karl-Morre-Straße 32

GPA Kärnten
9020 Klagenfurt, Bahnhofstraße 44/4

GPA Oberösterreich
4020 Linz, Volksgartenstraße 40

GPA Salzburg
5020 Salzburg,
Markus-Sittikus-Straße 10

GPA Tirol
6020 Innsbruck,
Südtiroler Platz 14

GPA Vorarlberg
6900 Bregenz, Reutegasse 11

www.gpa.at

GUTE ARBEIT!

mitgliedwerden.gpa.at

MEINE GEWERKSCHAFT