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

„Esoterische Kennzahlen auf Basis extensiver Verhaltens-analyse von Beschäftigten."

Wolfie Christl, tweet im Dezember 2020

„Der Kunde ist allein verantwortlich für alle Körperverletzungen oder Todesfälle, die durch den Einsatz vom Microsoft Teams und Anwendungen entstehen können."

Microsoft Volumenlizenzierung Online-Services-Bedingungen, November 2020, Seite 22

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

Stand: Februar 2021

GUTE ARBEIT!

AUTORIN

© Edgar Ketzer

Clara Fritsch
Gewerkschaft GPA – Abteilung
„Arbeit und Technik“

 Besonderheiten in der Welt von MS 365

 Zitate aus bestehenden (Muster-)Betriebsvereinbarungen zu MS 365

 Wichtige Hinweise zur Verwendung von MS 365

VORWORT

Der „Alleskönner" unter den Software-Giganten bietet Betriebssystem, Dokumentenverarbeitung, Kooperations- und Kommunikationstool – ob privat oder im Betrieb, in der Schule oder im Krankenhaus. Software von Microsoft ist aus den meisten Organisationen nicht mehr wegzudenken. Microsoft übernimmt immer mehr Aufgaben und wird immer leistungsstärker.

Gar viele Fragen stellen sich im Zusammenhang mit Microsoft 365 in der Cloud. Wer kann die höchst umfangreiche Software-Palette noch überblicken? Wer hat noch das notwendige Knowhow, um die unzähligen Apps, Features, Funktionen und Einstellungen von MS 365 kritisch zu begutachten? Unterscheiden sich die Microsoft-Anwendungen grundlegend von denen anderer Firmen? Gelten in der Cloud, also bei Software, die nicht direkt auf den betriebseigenen Servern liegt, andere Regeln als sonst? 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?

Die Marktmacht von Microsoft hat dazu geführt, dass sich auch die Gewerkschaft näher als ursprünglich gewünscht mit dem Konzern und seinen Produkten auseinandersetzen muss. Der Bedarf nach mehr Information, Auskunft und Erklärung zur Produktpalette „365" von Microsoft hat sich in den zunehmenden Anfragen der BetriebsrätInnen zu dem Thema gezeigt. Die Anfragen konnten mit Hilfe unserer bestehenden Unterlagen (z. B. Muster-Betriebsvereinbarungen, Broschüren, Rechtseinschätzungen) immer nur in Ausschnitten beantwortet werden. Eine neue Herangehensweise ist gefragt um BetriebsrätInnen der Gewerkschaft GPA bei der betrieblichen Verwendung von Microsoft-Produkten in der Cloud zu unterstützen. Es war an der Zeit, das vorliegende Werk in Angriff zu nehmen – wissend, dass es nie vollständig, geschweige denn abgeschlossen sein wird.

Hier liegt nun der Versuch einer Auskunft zum betrieblichen Einsatz von Microsoft 365 (MS 365) vor, der auch mit seinen vielen Querverweisen und den stark miteinander verzahnten Kapiteln die Welt von MS widerspiegelt und daher eine Struktur aufweist, die die alten Lesegewohnheiten über Bord wirft:

Folgende Kapitel geben einen generellen Ein- und Überblick zu MS 365: „Die Welt von Microsoft – was ist das Besondere an MS 365?" [S. 8], die „Interpretation von Beschäftigten-Daten – was macht MS 365?" [S. 11] und das Kapitel „Kritikpunkte aus Datenschutzsicht im Überblick" [S. 12].

Die nach unserer Erfahrung am meisten eingesetzten Produkte werden in den jeweiligen Unterkapiteln von „Die häufigsten Anwendungen von MS 365" [S. 30] dargestellt und die wichtigsten in einer Betriebsvereinbarung zu regelnden Punkte zu den einzelnen Anwendungen am Ende zusammengefasst.

Die grauen Kästchen enthalten – je nach Symbol (Legende auf der linken Seite) – wichtige Tipps und Hinweise für die Verwendung vom MS 365 beziehungsweise Zitate aus bestehenden Betriebsvereinbarungen.

Die Checklisten zum Schluss sollen dabei unterstützen, den Überblick bei der konkreten Gestaltung einer Betriebsvereinbarung (BV) zu behalten.

Viel Spaß beim Schmökern, Informationen sammeln und Umsetzen der Vorschläge in Betriebsvereinbarungen!

INHALT

DIE WELT VON MICROSOFT

WAS IST DAS BESONDERE AN MS 365?

Der Konzern Microsoft (MS) ist derzeit **Marktführer** in Sachen Unternehmens-Software und Betriebssysteme. Microsoft hat in den letzten Jahren besonders durch den Ausbau und den hohen Marktanteil von Büro-Software wie Office [S. 30] oder Outlook [S. 32] sowie durch sein Betriebssystem Windows einen Monopolstatus erreicht[1]. Besonders seit dem Corona-bedingten Shutdown im März 2020 und dem damit einhergehenden Arbeiten im Home-Office sind die diversen (lizenzfreien also gratis verfügbaren) Microsoft-Produkte deutlich häufiger im Einsatz.

MS 365 (ehemals „Office 365") ist seit Oktober 2010 auf dem Markt und umfasst ein sehr breites Angebot. MS 365 enthält unzählige einzelne Anwendungen, Apps, Funktionalitäten (z. B. Kalender, Kommunikation, Kollaboration, Security, Mobility, HR, Logistic, Finance, Marketing-Kampagnen, u.v.m.). Die meisten Ressourcen steckt Microsoft derzeit in den Ausbau der Kollaborations-Software Teams [S. 34]. Die Nachfrage ist hoch.

Die einzelnen Anwendungen werden **permanent optimiert**, verändert oder miteinander kombiniert. Anwendungen werden von anderen Unternehmen aufgekauft[2] oder neu erfunden und in die bestehenden integriert. Anwendungen werden mit anderen zusammengespielt oder auch nicht mehr weiterentwickelt und „versickern"[3]. Außerdem beinhaltet MS 365 Möglichkeiten zur Einbindung externer Apps/Programme/Anwendungen, wodurch die Sache noch unübersichtlicher wird.[4] MS 365 ist immer in Bewegung.

MS 365 kann auf unterschiedliche Art betrieben werden. NutzerInnen können die Anwendungen auf firmeneigenen Servern laufen lassen. Es gibt „Apps", also Programme, die aus der Cloud heruntergeladen und auch dort betrieben werden und es gibt Anwendungen, die auch ohne Installation auf lokal betriebenen oder mobilen Geräten, ausschließlich über das Internet, zur Verfügung stehen. MS 365 kann verwendet werden, ohne dass firmeneigene SystemadministratorInnen tätig werden oder firmeneigene Server erforderlich sind.

Unternehmen, die erstmals in die Welt von MS 365 einsteigen, lassen anfangs die eigenen Server oft zusätzlich zu denen in der Cloud mitlaufen. Bei der **Cloud-Variante** von MS 365 werden alle Daten auf Servern von MS gespeichert, wobei die verschiedenen NutzerInnen/Organisationen/Unternehmen/KundInnen nur auf ihre eigenen Datenbestände Zugriff haben (sollten). Die MS Server sind an unterschiedlichen Standorte verstreut und es ist nicht immer möglich, den tatsächlichen Speicherort ausfindig zu machen. Wenn Daten durch die NutzerInnen selbstständig verschlüsselt werden, kann es sein, dass auch MS nicht mehr feststellen kann,

1 https://netzpolitik.org/2018/wie-microsoft-europa-kolonialisiert/ ; 4.12.2020
2 https://www.derstandard.at/story/2000080902825/microsoft-kauft-github-fuer-7-5-milliarden-dollar
https://www.heise.de/news/Spieleindustrie-Microsoft-kauft-Bethesda-und-id-Software-4907190.html
3 https://www.heise.de/newsticker/meldung/Diese-Microsoft-Produkte-erreichen-am-14-Januar-das-Supportende-eine-Uebersicht-4636238.html; 16.12.2020
4 Eine aktuelle Übersicht über die vielfältige Produktpalette von MS 365 findet hier: https://github.com/AaronDinnage/Licensing ; 16.12.2020

auf welchen Servern die Daten physisch liegen. MS stellt daher ausschließlich organisatorisch sicher, dass andere NutzerInnen nicht auf fremde Datenbestände zugreifen – technisch ist es kaum zu kontrollieren. Das führte insbesondere aufgrund des In-Kraft-Tretens der Europäischen Datenschutzgrundverordnung (DSGVO) zu massiver Kritik, da Speicherorte auch außerhalb der EU lagen.

Um der Kritik entgegenzuwirken, werden seit Februar 2020 die Daten kommerzieller KundInnen von MS auf zahlreichen Serverfarmen innerhalb der EU-Grenzen gelagert, was allerdings nicht für alle Dienste gilt. Das Nachrichtenportal Heise hat recherchiert: *„Demnach liegen alle Daten zu Office Online (= Word, Excel, Powerpoint) einschließlich Teams, Exchange und Advanced Threat Protection (ATP) und SharePoint, Outlook, Mobile sowie Delve in Deutschland, Daten zum Chatdienst Yammer sowie fürs Azure Active Directory also Konto- und Konfigurationsdaten) jedoch unverändert auf Servern irgendwo im EU-Gebiet (vermutlich in Dublin oder Amsterdam). Lediglich bei Daten für My Analytics/Workplace Analytics und Sway bekennt Microsoft eine Speicherung in den USA."*[5]

AdministratorInnen haben in den Einstellungen zwar die Möglichkeit, ausschließlich Speicherorte innerhalb der EU auszuwählen, jedoch funktionieren dann einige Dienste nicht mehr (z. B. Sprachsteuerung für innerhalb der EU wenig gebräuchliche Sprachen).

Bei MS Cloud-Anwendungen wird die verwendete Software nicht mehr im eigenen Unternehmen installiert, gewartet, aktualisiert, repariert, ausgetauscht, ergänzt, Back-Ups erstellt, etc. Für die meisten Unternehmen liegt darin ein großer Vorteil, da viele zeit- und ressourcenintensive Aufgaben wegfallen; Personal, Speicherkapazitäten, IT-Knowhow, Updates, das alles stellt MS von sich aus zur Verfügung. Auch die Verfügbarkeit dürfte bei Cloud-Diensten verlässlicher und durchschnittlich besser gegeben sein, als bei den meisten firmenintern betriebenen Systemen. Gleiches gilt für die technische Sicherheit und Gefahrenabwehr („safety and security"), in die MS Kapazitäten investiert, die einer/m einzelnen NutzerIn im Regelfall nicht zur Verfügung stehen.

5 https://www.heise.de/newsticker/meldung/Microsoft-erweitert-sein-deutsches-Cloud-Angebot-4665168.html ; 04.12.2020

Natürlich fallen mit dem gebotenen Komfort Gestaltungsmöglichkeiten weg. Eine MS-Software, die vom Hersteller verwaltet wird, enthält maßgeschneiderte, vom Standard abweichende Einstellungen nur dann, wenn dafür – in Geld oder mit Daten – gezahlt wird.

Dass sämtliche Anwendungen in der Cloud laufen, hat den Nebeneffekt, dass sämtliche Nutzungsdaten (Metadaten, Telemetriedaten) bei MS landen. MS kann damit Vergleiche anstellen, Benchmarks erzeugen, alte Anwendungen „verbessern" und den Bedarf an neuen Anwendungsmöglichkeiten analysieren. Man kann davon ausgehen, dass dieser Datenschatz auch – im Rahmen geltender Gesetze – weiterverkauft wird.

Die Vorteile, die MS 365 den NutzerInnen bietet, liegen auf der Hand.

Die guten Eigenschaften von MS 3655

- MS funktioniert weitgehend stabil, weil sich die über den gesamten Erdball verteilten Serverfarmen bei Problemen gegenseitig ersetzen können.
- MS bietet ortsunabhängiges Arbeiten, indem die Server rund um die Uhr und von jedem Standort aus erreichbar sind und permanent gewartet werden.
- Raubkopien und unbefugte Lizenznutzungen sind kaum problematisch, weil alles auf MS-eigenen Rechnern betrieben wird und vieles ohnehin gratis angeboten wird.
- Kontinuierliche Zahlungen mittels Lizenzgebühren sind für Unternehmen besser planbar, als bei einmaligem Kauf (neuer) Software.
- Die KundInnen nutzen „maßgeschneiderte" Lösungen, weil der Bedarf ohnehin aufgezeichnet wird und aufgrund des genutzten Leistungsumfangs bekannt sind.
- Und nicht zuletzt profitiert MS auch von den vielen Metadaten, die ihnen NutzerInnen „zur Verbesserung der Dienste" zur Verfügung stellen.

Fast alle Anwendungen von MS 365 können auch auf mobilen Geräten installiert und ortsunabhängig verwendet werden, was zu der großen Beliebtheit von MS 365 beiträgt. Die Apps, die mobil verwendbar sind, haben allerdings weniger Anwendungen (z. B. kein „Publisher", womit Druckpublikationen, E-Mail-Headlines und Präsentationen erstellt werden können; kein „Forms", womit Umfragen und Quizze erstellt werden können) und einen geringeren Funktionsumfang als jene, die man in der Desktop-Version erhält (z. B. bieten weniger Schriftarten, erkennen Textbausteine von „Word" nicht, etc.). Die Apps, die ausschließlich über das Internet funktionieren, sind wenig nutzerfreundlich und für die berufliche Kooperation nicht so gut geeignet.

Je nachdem, welches MS-Abonnement ein Unternehmen gebucht hat, beziehungsweise, welche Lizenzen ein Unternehmen gekauft hat, unterscheidet sich das Angebot an verfügbaren Anwendungen und Erweiterungen. Es ist also sehr geräte- und betriebsabhängig, auf welche Art (wie), zu welchem Zweck (wozu), in welchem Ausmaß (wieviel) MS 365 jeweils verwendet wird. Es bestehen vielfältigste Kombinations- und Erweiterungsmöglichkeiten.

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 das Tool Graph [S. 38] verknüpft. Jede Anwendung von MS kreiert – egal ob von den NutzerInnen gewollt oder nicht – im Hintergrund Verbindungs- und Verhaltensdaten (sogenannte Metadaten oder Telemetriedaten). Dabei handelt es sich nicht nur um die Nutzungsdaten Einzelner (z. B. persönliche Einstellungen, individuelle Nutzungshäufigkeit, Präferenzen von Kommunikationszeitpunkten, etc.) sondern auch um die Beziehungen der einzelnen NutzerInnen untereinander (z. B. Reaktionsgeschwindigkeit anhand von Durchschnittswerten, Netzwerk an und Präferenzen zu KommunikationspartnerInnen, Position 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.[6]

MS 365 in der Cloud ist permanent online und übermittelt damit auch permanent bestimmte Daten an Microsoft, die „zur Verbesserung der Services" oder „zur technischen 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 von Interpretationen, die MS 365 vornimmt, die durchaus kritisch zu sehen sind[7]:

Werden während eines Meetings E-Mails von den Teilnehmenden versendet (über Outlook [S. 32] werden diese Daten protokolliert), führt das zu Auffälligkeiten (sog. „Findings") und wird als Treffen mit geringer Qualität („Low Quality Meeting") interpretiert.

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

Sind einem Termin keine weiteren TeilnehmerInnen zugeordnet, die aus den MS 365 Kontakten bekannt sind, wird der Termin als potentielle „Fokuszeit" gewertet. Das ist Zeit, die MS vorschlägt, um ungestört und konzentriert arbeiten zu können. Um die Fokuszeit festzustellen wird ausgewertet, wie „aktiv" jemand über einen bestimmten Zeitraum in einer Office-Anwendung gearbeitet hat. Dazu werden beispielsweise Tastenanschläge gemessen und mit der „Verweildauer" in einer bestimmten Anwendung in Beziehung gesetzt.[8] So schlägt MS auch Termine als potentielle „Fokuszeiten" vor, bei denen es sich beispielsweise um ein Webinar oder einen Arzttermin handelt.

Outlook [S. 32] nimmt eine durchschnittliche Zeit für das Verfassen eines E-Mails an, die nicht variabel ist und die nicht mit den realen Zeiten übereinstimmt. Weicht jemand von dieser Annahme ab, wird dies als ineffizient bewertet. Es wird also 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 mit anderen Personen aus den MS Kontakten wird dieser Umstand positiv beurteilt. KollegInnen mit hohem „Vernetzungsgrad" werden als „erfolgreicher" bewertet; wer kein ausgedehntes Netzwerk hat, gilt als weniger erfolgreich. In der beruflichen Praxis könnte ein hoher Interaktionsgrad aber genauso gut für einen hohen Grad an nicht-beruflicher Kooperation oder Unselbstständigkeit stehen. 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. Im Gegensatz zu der Erfolgsdefinition von MS, die vorrangig auf viel Vernetzung beruht, stehen ArbeitnehmerInnen, die permanent privat chatten, ebenso wie eigenständig arbeitende Fach-ExpertInnen, die wenig Schnittstellen zu anderen Beschäftigten oder Bereichen haben.

Theoretische Verlustrechnungen werden in Euro angeführt, ohne dass die genaue Berechnungsmethode offengelegt wird – ein Parameter dürften „uneffektive Meetings" sein (wie diese berechnet werden ist oben beschrieben).

---

6 Näher auseinandergesetzt mit dem Thema hat sich die Böckler Stiftung in ihrer Publikation aus der Reihe Mitbestimmungspraxis „Die Vermessung der Belegschaft".
7 Unter anderem zusammengestellt aus einer Präsentation von TIBAY (https://www.bildungswerk-bayern.de/tibay ; 09.12.2020) 2019 und einem Seminar von JES (https://www.jes-seminar.de/wir-sind-jes/ ; 09.12.2020).
8 https://www.boeckler.de/pdf/mbf_bvd_praxis_office_365.pdf

Mittels Künstlicher Intelligenz berechnet „My Analytics/ Workplace Analytics" [S. 39] seit 2020, wann die individuell besten Zeitfenster für „well-being" oder „focus time" bestehen[9], wobei die Berechnungsgrundlagen weitgehend im Dunkeln bleiben. My Analytics errechnet Ratschläge, wie beispielsweise „deaktivieren sie Arbeit außerhalb der Arbeitszeit". In der MS 365-Welt ist es sehr einfach, Arbeit außerhalb der Arbeitszeit zu erledigen, weshalb ein solcher Ratschlag durchaus passend sein kann. Gleichzeitig kann er aber auch sehr unpassend sein, wenn beispielsweise diese Trennung ohnehin erfolgt, von MS 365 aber ein privates E-Mail an ein/e KollegIn als „Arbeit" gewertet wird. Ohne die Berechnungsgrundlagen zu kennen, sind diese Empfehlungen folglich wenig aufschlussreich.

Die Benutzeranmeldung über „Azure Active Directory" [S. 44] schätzt ein, wo man sich gerade befindet, was dazu führt, 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.

MS 365 kann natürlich nur jene (Verbindungs-)Daten verarbeiten, die auf mit MS-eigenen oder mit MS verknüpften Apps erstellt werden. Arbeitet jemand mit einer Suchmaschine (z. B. duckduckgo), schreibt Nachrichten auf einer App (z. B. signal), benutzt einen Kalender (z. B. google calendar), postet auf Social-Media-Kanälen (z. B. Vero), leitet eine Videokonferenz (z. B. zoom), die *nicht* von MS stammt, können diese Aktivitäten auch nicht in die Interpretationen von MS einfließen. Arbeitszeit, die nicht mit MS Anwendungen verbracht wird, wird von MS als Inaktivität, Freizeit, oder Langsamkeit interpretiert. MS geht davon aus, dass sämtliche Arbeitsaktivitäten innerhalb der Welt der MS-Produktpalette laufen.

MS 365 errechnet also Zusammenhänge (Korrelationen), 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 statistisch wissenschaftlichen Grundprinzipien folgen.

Es entsteht ein pseudostatistischer Zusammenhang, den das Beratungsunternehmen TIBY wie folgt zusammenfasst: *„Jenseits der grundsätzlichen Problematik der Leistungs- und Verhaltenskontrolle besteht ein immenses Potential für fragwürdige Interpretationen der Analyseparameter."*

KRITIKPUNKTE AUS DATENSCHUTZSICHT IM ÜBERBLICK

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 als DSGVO-konform zu bezeichnen wäre.

Speicherfristen können nicht selbst 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 hingegen in vielen Belangen an die von MS vordefinierten Aufbewahrungsfristen gebunden (z. B. Speichern von Emails in Outlook [S. 30] oder von Aufnahmen in Teams [S. 34]).

Datenschutzfreundliche Voreinstellungen bzw. die Möglichkeit selbst definierte Einstellungen zum Datenschutz zu treffen, sogenannte „Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen", wie sie gemäß Artikel 25 DSGVO vorgeschrieben sind, bietet MS 365 nur in begrenztem Maße an.

MS behauptet, **Auftragsdatenverarbeiter** zu sein und somit seine Dienstleistungen ausschließlich für die Interessen der für die Datenverarbeitung Verantwortlichen, KundInnen und Unternehmen, zur Verfügung zu stellen (gemäß Art. 4 Z 8 DSGVO). MS betreibt aber gleichzeitig Auswertungen im eigenen Interesse, mitunter „selbstlernende" Systeme, die

9 https://www.microsoft.com/de-de/microsoft-365/blog/2019/05/06/minimize-distractions-stay-focused-ai-powered-updates-in-microsoft-365/

personenbezogene Daten der NutzerInnen verwenden (z. B. Bewertung von Telemetrie-Daten in Delve [S. 37] gesammelt in Graph [S. 38]; Beispiel zur Rechtschreibprüfung im MS-Programm Word siehe weiter unten).

Mit MS 365 ist es möglich, **Profile** über einzelne NutzerInnen zu erstellen. MS 365 erstellt diese Profile auf Basis intransparenter Parameter (z. B. My Analytics/ Workplace Analytics [S. 39]). Die Erstellung von Profilen erfolgt, ohne dass ausreichende **Informationen** an die Betroffenen erteilt werden. Zudem besteht die Gefahr, dass ArbeitgeberInnen auf der Grundlage der von MS verarbeiteten Daten, Entscheidungen gegenüber Beschäftigten 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), die aber gemäß Art. 35 DSGVO für bestimmte Anwendungen vom Verantwortlichen, also dem Unternehmen, vorgenommen werden müsste.

Es wurden und werden **Sicherheitslücken** festgestellt. So sind beispielsweise Daten unterschiedlicher Unternehmen (Clients) auf denselben Servern gespeichert und nur unzureichend voneinander getrennt (siehe weiter unten). Eigentlich müsste es aber geeignete Maßnahmen geben, um derartiges zu unterbinden (Art. 23 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, wegen des Machtgefälles zwischen ArbeitgeberIn und ArbeitnehmerIn, an echter Freiwilligkeit. Die Freiwilligkeit ist aber wesentlicher Bestandteil einer Zustimmung zur Datenverwendung gemäß Artikel 4 Z 11 DSGVO.

Immer wieder macht MS ungewollt Schlagzeilen mit seinem Geschäftsmodell und den darin auftretenden Sicherheitslücken. 2018 erhielt MS Deutschland den „BigBrotherAward“[10]. Die Fachzeitschrift „Computer & Arbeit“ widmete sich den Problemen bei MS 365 ausführlich in der Ausgabe 10/2019[11]. Bei der Übertragung von Telemetriedaten (das sind Verbindungs- und Nutzungsdaten) kommt es immer wieder zu Ungereimtheiten[12].

Beispiele für **Sicherheitslücken**, wenn MS Anwendungen nicht auf firmeneigenen Rechnern laufen, sondern in der Cloud (als sogenannte „SaaS; Software as a Service“) betrieben wird:

- Es werden Meta-Daten an Microsoft übertragen, bevor noch nach einer Einverständniserklärung beim Kunden /der Kundin gefragt wird.[13]
- Auch wurde festgestellt, dass das Login-Passwort im Klartext übermittelt wird (ebd.).
- Arbeitet man mit Office 365 Business Premium werden von IT-AdministratorInnen erstellte Gruppensicherheitsrichtlinien von MS nicht beachtet.[14] Beim teureren Lizenzvertrag „MS Enterprise“ treten diese Mängel nicht auf, wie der IT-Journalist Jürgen Schmidt herausgefunden hat (ebd.).
- Innerbetrieblich könnte man auf sämtliche Daten zugreifen, die in MS 365-Anwendungen erstellt werden, weil die Software permanent online ist und an Microsoft Daten übermittelt. Das haben IT-Experten mittels einer so genannten man-in-the-middle-Attacke ausprobiert und es ist ihnen „gelungen“.[15]
- Außerdem konnte es nicht ganz ausgeschlossen werden, dass andere ZertifikatsbesitzerInnen, also Unternehmen/KundenInnen bei Übertragungen mitlesen können.

10 https://bigbrotherawards.de/2018/technik-microsoft-deutschland ; 15.12.2020
11 https://www.bund-verlag.de/zeitschriften/computer-und-arbeit/archiv/2019_10 ; 15.12.2020
12 https://www.heise.de/select/ix/2019/5/1907710505118147453 ; 15.12.2020
13 https://www.datenschutz.saarland.de/ueber-uns/oeffentlichkeitsarbeit/detail/pressemitteilung-vom-02102020-stuttgart-muenchen-ansbach-wiesbaden-saarbruecken
14 https://www.heise.de/newsticker/meldung/Emotet-Sicherheitsrisiko-Microsoft-Office-365-4665197.html
15 https://www.heise.de/select/ix/2019/6/1911508530519573645

Die deutschen Datenschutzaufsichtsbehörden sind 2020 mehrheitlich übereingekommen, dass MS 365 an sich gar nicht DSGVO-konform[16] eingesetzt werden kann.[17] Einige Datenschutzbeauftragte aus deutschen Bundesländern haben dem Bericht allerdings nicht zugestimmt. Sie vertreten die Meinung, dass man MS 365 nicht generell beurteilen könne, da es ein komplexes System, zusammensetzt aus vielen unterschiedlichen Anwendungen, sei.[18] Stefan Brink, der Landesbeauftragte für Datenschutz und Informationsfreiheit in Baden-Württemberg, kritisierte bereits vor dem Beschluss der deutschen Behörden die Kommunikationsmöglichkeiten von MS 365, da er die Datenschutzfolgenabschätzung[19] des Kultusministeriums zur Nutzung von Microsoft Office 365 an Schulen, gelesen hatte: „Es scheinen derzeit strukturelle Merkmale der ins Auge gefassten Verarbeitung vorzuliegen, welche die Möglichkeit eines datenschutzkonformen Einsatzes ohne wesentliche Anpassung der Datenverarbeitung durch Microsoft fraglich erscheinen lassen (...) Datenschutzrechtlich stellt der Abfluss personenbezogener Daten zu Microsoft zu eigenen Zwecken des Anbieters eine Übermittlung dar, für die eine Rechtsgrundlage nicht ersichtlich ist."[20] Welche konkreten Folgen aus der Diskussion abgeleitet werden, ob Strafen verhängt werden oder ob es zu eindeutigen Empfehlungen kommen wird, ist zum Zeitpunkt der Fertigstellung dieser Publikation im Dezember 2020 noch nicht entschieden.

MS bemüht sich laufend um Verbesserungen[21]. In den letzten beiden Jahren wurde beispielsweise das Tool „Diagnosedatenanzeige" erstellt, mittels dem NutzerInnen wenigstens prüfen können, welche Telemetrie-Daten an MS weitergegeben werden.

Allerdings waren nicht alle Bemühungen um mehr Privatsphäre und Datenschutz von Erfolg gekrönt. Der Programmierer, Forscher und Netzaktivist Wolfie Christl[22] sowie der Datenschutz-Experte des Deutschen Gewerkschaftsbundes[23] und die Österreichische Arbeiterkammer[24] sind davon überzeugt, dass einige Werkzeuge von MS 365, insbesondere Workplace Analytics [S. 39], nicht DSGVO-konform sind. Bertold Brücher, Rechtsexperte beim DGB, erklärte gegenüber dem Magazin „c't"[25] im November 2020: „Funktionen, mit denen Unternehmen die Arbeitsgepflogenheiten ihrer Bürobelegschaft detailliert durchleuchten können, widersprechen und verstoßen gegen Persönlichkeitsrechte der Mitarbeiter, Datenschutz und – wenn vorhanden – den Beteiligungsrechten und -pflichten der Betriebs- oder Personalräte." MS hat sich kurz nach dem medial äußerst hohen Interesse für das kritisierte Feature entschuldigt[26], sich bei Wolfie Christl für seine Aktivitäten bedankt und lässt nun nur mehr zusammengefasste Auswertungen auf Analytics zu, bei denen die Namen der einzelnen Beschäftigten anonymisiert sind. Der „Produktivitätsscore" ist aber nach wie vor im Einsatz und die dahinterliegenden Datensammlungen ebenso.

Ein weiterer Kritikpunkt ist die Sache mit dem „Auftragsdatenverarbeitervertrag". Wenn ein Unternehmen oder eine Person Produkte von MS 365 verwenden möchte, braucht es einen Vertrag mit MS, der klarstellt, zu welchen Bedingungen die MS-Programme genutzt werden dürfen, einen Auftragsdatenverarbeitervertrag (AVV). MS stellt einen solchen Vertrag unter dem Titel „Office Service Terms, OST"[27] online zur Verfügung und aktualisiert ihn fortwährend[28]. MS sieht sich in diesem Vertragsverhältnis als reiner Auftragsdatenverarbeiter im Sinne der DSGVO, was bedeutet, dass Programme nur bereitgestellt und Daten ausschließlich für andere verarbeitet würden. MS stünde demnach ausschließlich im Auftrag der „Verantwortlichen" (also rein für die KundInnen/Unternehmen/Lizenzvertragsinhaber-Innen) und deren Verwendungszwecke zur Verfügung und würde die Daten nicht für eigene Zwecke verarbeiten (Artikel 29 DSGVO).

16 https://www.heise.de/news/Microsoft-Office-365-Die-Gruende-fuer-das-Nein-der-Datenschuetzer-4919847.html ; 15.12.2020
17 https://www.heise.de/news/Microsoft-Office-365-Die-Gruende-fuer-das-Nein-der-Datenschuetzer-4919847.html
18 https://www.golem.de/news/office-365-warum-microsoft-die-datenschuetzer-spaltet-2010-151315-2.html
19 https://www.baden-wuerttemberg.datenschutz.de/lfdi-begleitet-pilotprojekt-des-kultusministeriums-zur-nutzung-von-microsoft-office-365-an-schulen/; 15.12.2020
20 https://www.badische-zeitung.de/eisenmann-setzt-auf-microsoft-plattform-fuer-schulen-und-erntet-kritik--189022089.html
21 https://www.microsoft.com/en-us/microsoft-365/blog/2019/05/01/microsoft-office-new-privacy-controls/ ; 15.12.2020
22 https://twitter.com/WolfieChristl/status/1331221942850949121 ; 15.12.2020
23 https://www.heise.de/news/Anwenderueberwachung-durch-Microsofts-Office-Software-4968615.html ; 15.12.2020
24 https://apps.derstandard.at/privacywall/story/2000121939043/microsoft-365-gibt-firmen-umfassende-moeglichkeiten-zur-ueberwachung-ihrer- mitarbeiter ; 15.12.2020
25 https://www.heise.de/news/Anwenderueberwachung-durch-Microsofts-Office-Software-4968615.html ; 15.12.2020
26 https://www.theguardian.com/technology/2020/dec/02/microsoft-apologises-productivity-score-critics-derided-workplace-surveillance ; 15.12.2020
27 https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=18335 ; 15.12.2020
28 https://www.microsoft.com/licensing/terms/product/changes/EAEAS ; 15.12.2020

Die niederländische Datenschutzbehörde[29] wollte 2018 Office 365 ProPlus, Windows 10 Enterprise und Office 365 online zur Datenverarbeitung einsetzen und prüfte daher vorab mittels einer Datenschutzfolgenabschätzung. Sie kam zu dem Schluss, dass diese Anwendungen von MS nicht der DSGVO entsprechen. Die Datenschutzfolgenabschätzung der niederländischen Behörden[30] zu Office 365 hat ergeben, dass MS bis zu 23.000 „Ereignisse" ohne nähere Zweckbestimmung, ohne Information an die Betroffenen und ohne Auftragsverarbeitervertrag in die USA übermittelt hat. Ein solches „Ereignis" war beispielsweise die Autokorrekturfunktion des Rechtschreibprogramms von „Word", die automatisch „mitlernt" und alle vorgenommenen Korrekturen samt IP-Adresse speichert. Als Rechtsgrundlage im Sinne der DSGVO wurde von MS ein „berechtigtes Interesse" angegeben. Abgesehen davon, dass es fragwürdig ist, wozu IP-Adressen-Speicherung hier benötigt wird, steht ein solches Interesse einem Auftragsverarbeiter aber nicht zu. Der Auftragsverarbeiter verarbeitet Daten schließlich nur im Auftrag. Ein Auftragsverarbeiter müsste die NutzerInnen über solche Datenverwendungen im eigenen Interesse informieren, was nicht erfolgt ist. Eine Speicherung sämtlicher IP-Adressen zum Mitlernen bei Autokorrekturen steht wohl kaum im direkten Interesse der Unternehmen, die MS-Lizenzen gekauft haben, geschweige denn der NutzerInnen. Da hat MS wohl bei Office 365 die Daten im eigenen Interesse weiterverarbeitet.

MS 365 beinhaltet also auch Funktionen, die die Aktivitäten von NutzerInnen permanent überwachen und die personenbezogene Daten beim Mutterkonzern in den USA speichern.

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 bei vielen Funktionen keine Möglichkeit, selber zu gestalten („Privacy by default") bzw. sie effektiv abzuschalten („Opt-Out") – es fehlen also datenschutzfreundliche Einstellungen.

29 https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise : 15.12.2020
30 https://www.privacycompany.de/datenschutz-folgenabschatzung-zeigt-risiken-bei-microsoft-office-proplus-enterprise/ ; 15.12.2020

HANDLUNGS-MÖGLICHKEITEN DES BETRIEBSRATES

Aus dem **Arbeitsverfassungsgesetz** ergeben sich für den Betriebsrat viele Möglichkeiten, wie er sich bei der Gestaltung von MS 365 einbringen kann.

- Der Betriebsrat kann ins Feld führen, dass die Einhaltung von gesetzlichen Vorgaben überwacht werden muss (z. B., wenn er/sie Einsicht in Auswertungen nehmen will).

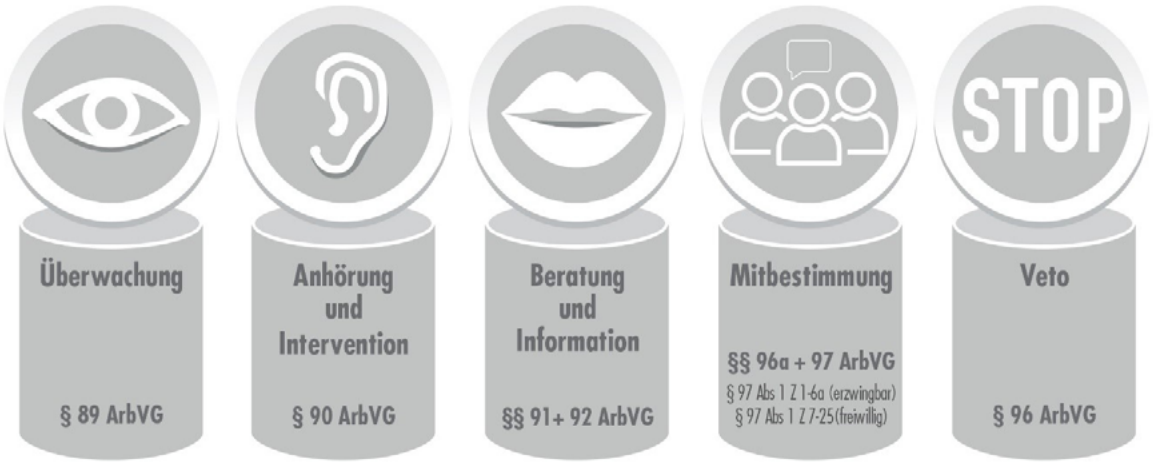
- Er kann eine Anhörung verlangen, bei der Vorschläge zur Gestaltung einzelner Anwendungen gemacht werden (z. B. Präsenzstatus ausschalten).

- 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 Technische Checkliste zum Einsatz von Microsoft 365 [S. 50] und die Checkliste, was in einer (Basis-)Betriebsvereinbarung zu regeln ist [S. 51]).

- Er kann den Abschluss einer Betriebsvereinbarung durchsetzen.

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

INSTRUMENTE DES BETRIEBSRATS



Quelle: Gewerkschaft GPA

DIE ARBEITSVERFASSUNGSRECHTLICHE EINORDNUNG IM DETAIL

Das österreichische Arbeitsverfassungsrecht sieht hinsichtlich zahlreicher Fragen Mitwirkungsrechte des Betriebsrats vor. So gibt die zentrale Bestimmung des § 96 Abs 1 Z 3 ArbVG vor, dass „*die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, sofern diese Maßnahmen (Systeme) die Menschenwürde berühren*", zu ihrer Rechtswirksamkeit der Zustimmung des Betriebsrates bedürfen. Man spricht diesbezüglich von einer „**notwendigen Betriebsvereinbarung**".

Besteht in einem Unternehmen kein Betriebsrat, so schreibt § 10 AVRAG vor, dass in diesem Fall die Einführung (und Nutzung) von Kontrollmaßnahmen und technischen Kontrollsystemen, welche die Menschenwürde berühren, von der Zustimmung des betroffenen Arbeitnehmers/der betroffenen Arbeitnehmerin abhängig ist. Es muss also jeder/jede MitarbeiterIn, die einer derartigen Kontrolle unterworfen werden soll, zustimmen.

Die Begriffe der „Kontrollmaßnahme" bzw. des „technischen Systems zur Kontrolle der Arbeitnehmer" sind im weiten Sinne zu verstehen. Es kommt dabei nicht auf eine subjektive Absicht zur Überwachung durch den/die ArbeitgeberIn an, sondern auf eine objektive Eignung der Maßnahme bzw. des Systems zur Kontrolle. Die bloße Möglichkeit zur Kontrolle reicht also aus. 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.

Daneben bietet das ArbVG eine weitere Grundlage für den Abschluss einer Betriebsvereinbarung. Danach bedürfen 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) der Zustimmung des Betriebsrates.

Stimmt der Betriebsrat nicht zu, kann die Zustimmung zu einer Betriebsvereinbarung auf Grundlage des § 96a ArbVG durch eine Entscheidung der Schlichtungsstelle ersetzt werden („**ersetzbare Zustimmung**").

Obwohl das Gesetz jeweils von der „Einführung" bestimmter Maßnahmen oder Systeme spricht, ist darunter auch die Erweiterung, Weiterentwicklung bzw. teilweise Rücknahme bereits bestehender Maßnahmen oder Systeme zu verstehen. Werden beim Einsatz von MS 365 also substantielle Updates vorgenommen, so darf dies jeweils nur nach Zustimmung des Betriebsrates geschehen.

Ist sowohl nach § 96, als auch nach § 96a ArbVG eine Betriebsvereinbarung abzuschließen, geht die stärkere Mitbestimmungsvorschrift vor, also § 96 ArbVG. In derartigen Fällen kann die Zustimmung des Betriebsrates nicht durch eine Entscheidung der Schlichtungsstelle ersetzt werden.

Angesichts der geradezu lückenlosen Aufzeichnung des persönlichen Nutzungsverhaltens durch MS 365-Produkte, in die teilweise auch Vorgesetzte Einsicht haben können, ist tendenziell davon auszugehen, dass eine Betriebsvereinbarung gemäß § 96 Abs 1 Z 3 ArbVG abzuschließen ist. Darüber hinaus werden in vielen Fällen personenbezogene Daten ermittelt bzw. an Microsoft übermittelt.

DATENSCHUTZRECHTLICHE FRAGESTELLUNGEN

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 EU-Datenschutzgrundverordnung und des Datenschutzgesetzes (DSG) zur Anwendung gelangen.

Betroffenenrechte – Auskunft, Berichtigung, Löschung

Personen, deren persönliche Daten von Anderen verarbeitet werden, haben eine Reihe von individuellen Rechten zur Durchsetzung des Grundrechts auf Datenschutz (§ 1 DSG), welches sich u.a. aus dem Recht auf Schutz der Privatsphäre (Art. 8 EMRK) ergibt, darunter insbesondere die Rechte auf Auskunft, Berichtigung und Löschung (Art. 15 ff DSGVO).

Betroffene, also auch Beschäftigte, die MS-Anwendungen nutzen, haben Anspruch auf Auskunft darüber, wer welche (Kategorien) ihrer personenbezogenen Daten zu welchem Zweck und auf welcher Rechtsgrundlage, für welchen Zeitraum aufbewahrt bzw. speichert und gegebenenfalls auf welchem Wege die Daten an den/die Verantwortliche/n gelangt sind sowie an welche Empfängerkreise die Daten weitergegeben werden bzw. worden sind. Der/die Verantwortliche hat auf ein solches Auskunftsbegehren binnen vier Wochen Auskunft zu geben.

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

Zudem kann die betroffene Person verlangen, dass die sie betreffenden personenbezogenen Daten unverzüglich gelöscht werden, soweit dem keine rechtliche Verpflichtung zur Aufbewahrung entgegensteht und die Aufbewahrung für die Zwecke, für die sie erhoben wurden, nicht mehr zutreffen oder die Rechtsgrundlage der Verarbeitung fehlt oder die Daten von Beginn an unrechtmäßig verarbeitet wurden.

Aufbewahrung & Löschung

Ganz grundsätzlich dürfen Verantwortliche die personenbezogenen Daten Anderer 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 Daten unabhängig von einem entsprechenden Begehren der betroffenen Person regelmäßig zu löschen. Um dieser Pflicht nachzukommen empfiehlt es sich in regelmäßigen Abständen automatisierte Löschvorgänge einzurichten bzw. Löschroutinen zu etablieren.

Übermittlung von Daten (in einen Drittstaat) und Auftragsdatenverarbeitervertrag

Unternehmen müssen personenbezogene Daten nicht zwangsläufig selbst verarbeiten, sondern können auch auf (Sub-)Unternehmen zurückgreifen, die Datenverarbeitungen in ihrem Auftrag für sie vornehmen. Derartige beauftragte Unternehmen werden in der Terminologie der DSGVO als „Auftragsdatenverarbeiter" bezeichnet. Die Übermittlung von personenbezogene Daten an externe Auftragsdatenverarbeiter bedarf (ebenso wie jeder andere Verarbeitungsvorgang) einer Rechtsgrundlage, in diesem Fall eines Auftragsdatenverarbeitungsvertrages (AVV). Dieser dient dazu, die Rechte und Freiheiten der von der Datenverarbeitung betroffenen Personen zu schützen und muss daher Art und Zweck, Speicherdauer sowie die Pflichten des/der Verantwortlichen sowie des/der AuftragsdatenverarbeiterIn festlegen. Im Hinblick auf den Einsatz von MS 365 erscheint es wohl geboten, zwischen dem/der ArbeitgeberIn und Microsoft einen AVV zu schließen, um die an Microsoft übermittelten personenbezogenen Daten der Beschäftigten angemessen zu schützen.

Problematisch ist die Tatsache, dass Microsoft die umfangreich erhobenen personenbezogenen Daten österreichischer NutzerInnen in die USA übermittelt. Eine Grundlage dafür bildete seit 2016 das „**Privacy Shield-Abkommen**" zwischen den USA und der EU, welches den USA ein mit der EU vergleichbares Datenschutzniveau bescheinigte. Mit einer weitreichenden Entscheidung des Europäischen Gerichtshofes (EuGH 16.07.2020, C-311/18, Rechtsache Schrems II) wurde diese Praxis für unzulässig erklärt.

Sollen personenbezogene Daten in den Drittstaat USA übermittelt werden, kann alternativ nun insbesondere auf die sogenannte „**Standarddatenschutzklauseln**" der EU-Kommission zurückgegriffen werden. Wie der EuGH in seinem Urteil andeutet, kann jedoch, auch unter Nutzung der Standarddatenschutzklauseln, nicht schon von vornherein davon ausgegangen werden, dass den Grundsätzen der DSGVO genüge getan ist. Der/Die ÜbermittlerIn 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, was auch bei der Nutzung von Microsoft-Produkten, bei denen eine solche Übermittlung stattfindet (z. B. Sway und MyAnalytics [S. 39]) im Arbeitskontext berücksichtigt werden sollte.

Datenschutzfolgenabschätzung (DSFA)

Zusätzlich zum Mitbestimmen bei einer Betriebsvereinbarung ist der Betriebsrat auch bei der Datenschutzfolgenabschätzung einzubeziehen (Art. 35 DSGVO). Dabei sollte vorab in einer so genannten „**Schwellenwertanalyse**" das Risiko, das den Anwendungen innewohnt, eingeschätzt werden. „Wird bei der Nutzung der Systeme in die Privatsphäre der Beschäftigten eingegriffen?", lautet die maßgebliche Frage bei einer solchen Risikoanalyse.

Ist das Risiko hoch, dass die Privatsphäre der Beschäftigten beeinträchtigt wird, muss der/die ArbeitgeberIn eine Datenschutzfolgenabschätzung durchführen. 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 Betroffen zu erkennen, Gegenmaßnahmen zu ergreifen und nicht zuletzt das durch Datenschutzverletzungen entstehende wirtschaftliche Risiko zu minimieren. Eine rückblickende Regulierung ist im Datenschutz schwer möglich – passiert eine Rechtsverletzung, ist es bereits zu spät.

Bei der DSFA ist der/die **betriebliche Datenschutzbeauftragte** beizuziehen. Zusätzlich sind die **Standpunkte der Betroffenen und ihrer Vertretung** anzuhören. Dem Betriebsrat kommt im Rahmen der DSFA also eine wichtige Rolle zu. Rechtlich verantwortlich für die Durchführung der DSFA ist dennoch der/die ArbeitgeberIn.

Gerade künstliche Intelligenz, systematische Auswertung des persönlichen Verhaltens der NutzerInnen und die Verknüpfung großer Mengen von Daten, wie sie bei MS 365 typischerweise Bestandteile des Systems sind, setzen eine DSFA voraus.

Die Gewerkschaft GPA hat Tipps zusammengestellt, welche Prüfschritte und Fragestellungen für die Datenschutzfolgenabschätzung und die Beteiligung des Betriebsrates relevant sind.[31]

Um MS 365 in Betrieben einsetzen zu können, braucht es also eine **Betriebsvereinbarung** gemäß Arbeitsverfassungsgesetz. Die DSGVO ermöglicht ebenso, dass eine BV 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...*" (Artikel 88 DSGVO). ArbVG und DSGVO ergänzen einander diesbezüglich.

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

31 Diese erhaltet ihr bei den betriebsbetreuenden RegionalsekretärInnen.

DIE ERSTELLUNG EINER BETRIEBSVEREINBARUNG

Nahezu alle Anwendungen von MS 365 bedürfen einer **Betriebsvereinbarung**. Die vielen Kombinations- und Auswertungsmöglichkeiten (siehe Graph [S. 38]) und Interpretation von Beschäftigten-Daten [S. 11]) machen eine oder mehrere maßgeschneiderte Betriebsvereinbarungen erforderlich.

Die Empfehlung an BetriebsrätInnen lautet daher, sich genau anzusehen, welche Teile von MS 365 konkret verwendet werden (siehe Technische Checkliste zum Einsatz von Microsoft 365 [S. 52]) und dann gezielt zu den Anwendungen, die im Betrieb im Einsatz sind, die jeweils passende Musterbetriebsvereinbarung der Gewerkschaft GPA als Inspirationsquelle für konkrete Formulierungen heranzuziehen. Die Gewerkschaft GPA bietet zahlreiche Muster-BV zu einzelnen Systemen wie E-Mail/Internet, Telefonsysteme, Videokonferenzsysteme, Mobile Device Management, etc.

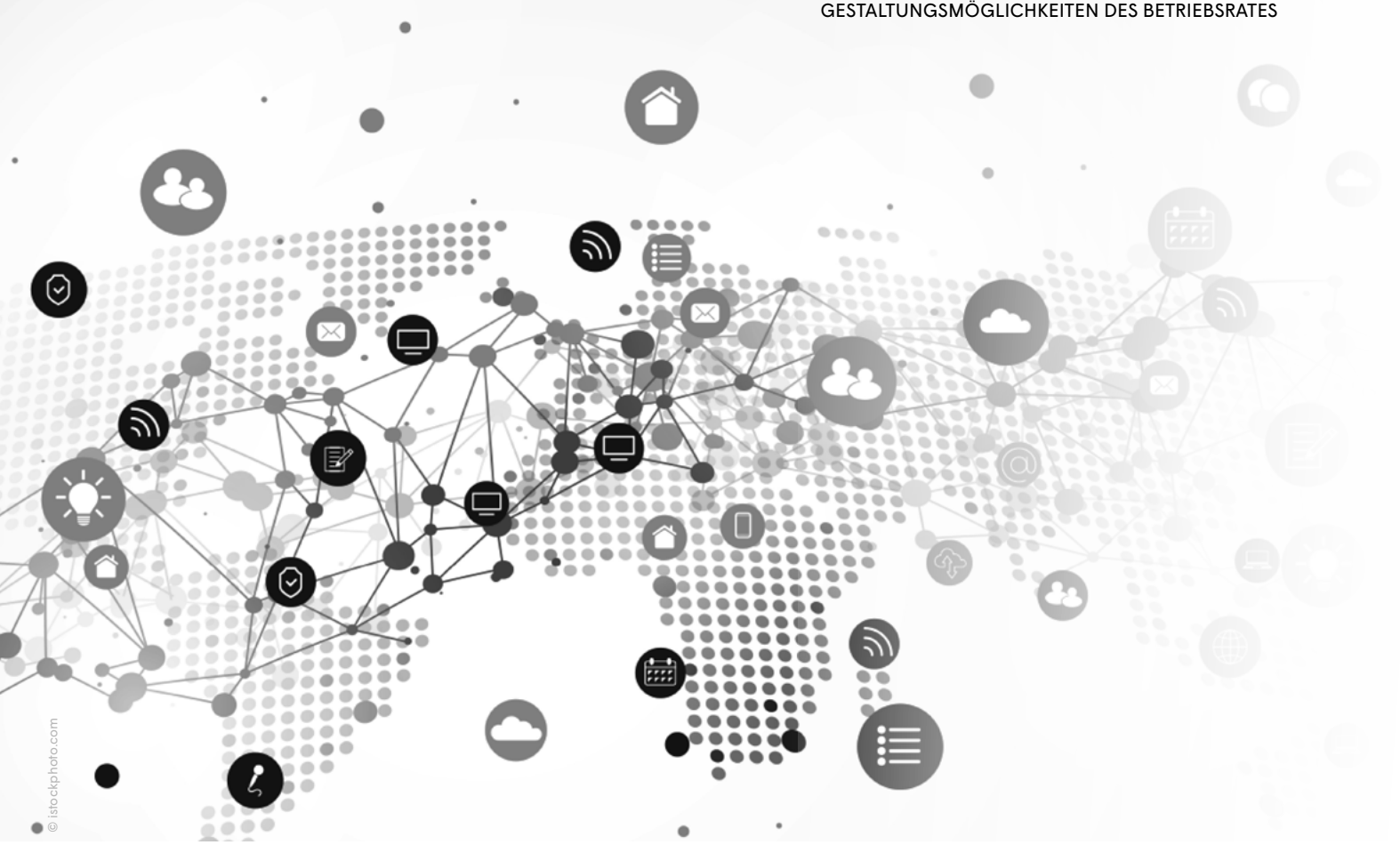
Die Verwendung vieler unterschiedlicher Systeme und mannigfaltiger Beschäftigtendaten generell „unter einen Hut zu bringen" könnte am besten mit Hilfe der „*Rahmen-Muster-BV Datenschutz*" klappen. Diese Rahmen-BV der Gewerkschaft GPA enthält Datenschutzregelungen, die für sämtliche Systeme gelten (z. B. der Umgang mit Protokolldaten, die in allen Systemen anfallen und rein technisch eine umfangreiche Verhaltensüberwachung ermöglichen). Man wird sich die jeweils zum Betrieb passende Betriebsvereinbarung selbst zusammenstellen müssen – so wie auch jeder Betrieb aus den unterschiedlichsten MS 365 Anwendungen ein eigenes System „zusammenpuzzelt".

DIE ENTSCHEIDUNG DES BETRIEBSRATES

Der BR muss abwägen, ob er den betrieblichen Einsatz einer MS 365 Anwendung unterbinden möchte, indem er den Abschluss einer BV verweigert. Damit ist in der Regel der Einsatz der jeweiligen Anwendung rechtskonform nicht mehr möglich. Dabei kann sich der Betriebsrat auf die Argumentation aus den Kapiteln Interpretation von Beschäftigten-Daten – Was macht MS 365? [S. 11] und Kritikpunkte aus Datenschutzsicht im Überblick [S. 12] stützen.

Die andere Variante ist, dass der Betriebsrat mit dem Abschluss einer Betriebsvereinbarung bestmöglich auf die Verwendung von MS 365 Einfluss nimmt. In der BV können durch Festlegungen und klare Regeln Auswertungen minimiert werden und eine überschießende Leistungskontrolle der Beschäftigten zumindest teilweise unterbunden werden, kurzum, es kann das Durchleuchten der Beschäftigten hintangehalten werden.

Selbst, wenn eine BV zustande kommt, so verringert diese nicht die grundsätzliche datenschutzrechtliche Verantwortlichkeit, die bei dem/der ArbeitgeberIn liegt. Das Bestehen einer Betriebsvereinbarung ändert nichts daran, dass die EU-Datenschutzgrundverordnung (DSGVO) und das Datenschutzgesetz (DSG) angewendet werden müssen. Eine BV kann die datenschutzrechtlichen Mängel von MS 365 nicht beseitigen.



Die wichtigsten Fragen zur Betriebsvereinbarung

Schritt eins beim Einsatz von MS 365 ist es, sich einen Überblick über Anwendungen im Betrieb zu verschaffen. Die Technische Checkliste zum Einsatz von Microsoft 365 [S. 52] hilft dabei.
▸ *WELCHE MS 365 Anwendungen werden verwendet?* lautet die Frage, die sich der BR stellen muss.

Schritt zwei ist es, den Zweck der Verwendung festzustellen (z. B. Personalverwaltung, Kommunikation, mobiles Gerätemanagement, Sicherheitsvorkehrungen, etc.).
▸ *WOZU sollen die MS 365 Anwendungen verwendet werden?* lautet die Frage, die sich der BR stellen muss.

Auf dieser Basis folgt erst **Schritt drei** bei dem die BV erstellt wird. Dazu können die Anregungen und Beispieltexte dieser Broschüre oder passender Abschnitte aus den Muster-Betriebsvereinbarungen der Gewerkschaft GPA gewählt werden. Die Muster-BVen liefern Anhaltspunkte und Vorschläge, wie die Module im Betrieb konkret zum Einsatz kommen sollen. Die Checkliste, was in einer (Basis-)Betriebsvereinbarung zu regeln ist [S. 51] 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 SOLLTE MS 365 GEREGELT WERDEN?

Beim Arbeiten mit MS 365-Produkten sollten einige grundlegende Gestaltungsvorschläge beachtet werden, unabhängig davon, welche Programme, Lizenzen, Anwendungen, Services, etc. genutzt werden (Überblick dazu bietet die Checkliste, was in einer (Basis-)Betriebsvereinbarung zu regeln ist) [S. 51].

Die **Zweckbindung** muss eindeutig sein. Es muss klar ersichtlich sein, welche Daten wofür verwendet werden (z. B. Speichern von Sprachnachrichten um gesetzliche Haftungsansprüche klären zu können).

Beispiel aus einer BV-Präambel: Die Betriebsvereinbarung dient dazu, die Interessen der ArbeitnehmerInnen zu wahren, ihre Persönlichkeitsrechte, ihrer Privatsphäre und ihre Gesundheit zu schützen. Die Software wird eingesetzt um eine stabile und sichere Verwaltung der Personaldaten zu gewähren und eine mobile Kommunikation zu gewährleisten. (Anm.: in dem Betrieb wurden in der BV Office (= Word, Excel, Powerpoint) [S. 30] und Teams [S. 34] geregelt)

Aus der Zweckbindung ergibt sich, wer welche **Berechtigung** erhalten muss. Berechtigungskonzepte sind äußert restriktiv zu fassen, damit die ohnehin weit verflochtenen Datenkombinations- und Auswertungsmöglichkeiten keinen allzu großen Einblick in das Verhalten und die „Leistung" der Beschäftigten ermöglichen. Innerhalb des Berechtigungskonzeptes von MS 365 können in etwa 50 fixe Zugriffsberechtigungen, so genannte „Rollen" vergeben werden. Der Betriebsrat sollte jedenfalls sicherstellen, dass er zur Überprüfung der BV auch eine umfassende „Rolle" erhält.

Die Rollenbezeichnung „globaler Leser" ermöglicht es, sämtliche Aktivitätsprotokolle von MS 365 zu sehen. Nicht möglich ist damit das Abändern, die Einsicht in (potentiell persönliche) Inhalte oder selbständiges Gestalten der Protokolle. Die Rolle eignet sich somit gut für die Betriebsratsarbeit. Der BR sollte sie sich verschaffen.

Manche Funktionen in MS 365 bauen auf langfristig auswertbaren personenbezogenen Datenhistorien auf (s. Delve [S. 37], Graph [S. 38]). Die gesetzliche Vorgabe für Löschfristen wird durch diese Funktionen konterkariert. Innerbetrieblich muss aber zumindest ein Vorgehen vereinbart werden, damit man nicht mehr benötigte Daten „Außer-Betrieb-Nehmen" kann bzw. diese nicht mehr eingesehen, ausgewertet, verglichen etc. werden[32].

32 D.h. „Recht auf Einschränkung der Verarbeitung" gem. Artikel 18 DSGVO

Auch wenn die technische Möglichkeit zu langen 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. Schon alleine, damit den Vorgaben der Datenschutzgrundverordnung, die verlangt, dass „technische und organisatorische Maßnahmen" getroffen werden (gem. Art. 32 DSGVO), Folge geleistet wird.

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

Die in MS 365 erzeugten Verhaltensdaten dürfen für operative Zwecke in konkreten Einzelprojekten genutzt werden, nicht jedoch zur gezielten systematischen Auswertung.

Die Einstellung im Benutzerkonto „optional verbundene Erfahrungen" in der Rubrik „Datenschutz" müsste deaktiviert werden, um das Anzeigen unerwünschter Datensammlungen einzuschränken. Die Auswertungen erfolgen dann zwar immer noch, werden aber den NutzerInnen nicht mehr angezeigt. Auswertungen können also nur bedingt verhindert werden.

Empfehlenswert ist es, die **Privatnutzung** zu regeln. MS 365 ermöglicht eine Nutzung, die weit über betriebliche Zwecke hinausgeht. Daher sollte der/die ArbeitgeberIn klar kommunizieren, was in der Arbeitszeit verboten ist (z. B. Games, Filme, Shoppen ...) und was erlaubt ist. Für die Privatnutzung sollte festgelegt sein, wo gespeichert wird (z. B. private Daten nur lokal im Gerätespeicher; betriebliches nur in der dafür vorgesehenen Cloudapplikation).

Vorschlag für eine Formulierung zur Privatnutzung in einer BV: 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.

Eine unglaubliche Menge von Tools und Plattformen stehen im Rahmen von MS 365 zur Verfügung. MS 365 bietet zusätzlich **Schnittstellen** zu externen Programmen wie z. B. der Spiele- und Softwareplattform „Steam". Auf all diesen Applikationen, Anwendungen und Softwareprogrammen können sämtliche Aktivitäten der NutzerInnen gespeichert, nachverfolgt und ausgewertet werden. Somit können tiefgreifende, in die Privatsphäre reichende Persönlichkeitsprofile erstellt werden.

Wird MS 365 in der **Cloud** eingesetzt, werden sämtliche Daten in der Cloud, also auf den Servern des Betreibers MS gespeichert. MS spielt sie mit denen anderer KundInnen zusammen, aggregiert sie und hat somit die Möglichkeit, die Daten (im Rahmen der Nutzungsbedingungen) maschinell zu analysieren – und der ArbeitgeberInnenseite in neuer Form anzubieten. Es wäre sinnvoll, derartig umfassende und angereicherte Datenanalysen (auch „Data Mining" genannt) durch Dritte auszuschließen. Aufgrund der zahlreichen Auswertungsmöglichkeiten von Daten, die MS bei Nutzung in der Cloud speichert, ist es besser, bestimmte Daten nicht in der cloudbasierten Anwendung von MS zu verwenden, sondern „on premise" (lokal, auf eigenen Servern) abzuspeichern.

Beispieltext aus einer BV: Besonders schützenswerte und vertrauliche Daten, insbesondere Gesundheitsdaten, sollen auf zentralen Netzwerk-Speicherorten („on premise") abgespeichert werden.

Der Betriebsrat des Deutschen Senders NDR hat durchgesetzt, dass Outlook [S. 32] vorerst nicht als Cloud Lösung eingesetzt wird. „*Wir werden auch Outlook ‚on premise' stellen, d. h. die Software wird auf einem Server im eigenen Unternehmen installiert. Die große Microsoft-Cloud zur Ablage unserer Daten benutzen wir noch nicht*" erklärte die Vorsitzende.[33] Diese Vorgehensweise ist also möglich.

Damit die Unzulänglichkeiten von MS 365 nicht zu Lasten der Beschäftigten gehen, sollten eindeutige und klare **Ziele** und **Prinzipien** in einer BV festgehalten werden (z. B. in einer Präambel):

- der Schutz der **Privatsphäre** der Beschäftigten
- **Transparenz** und Datensparsamkeit bei der Ermittlung, Verarbeitung und Übermittlung personenbezogener Daten (nach Art. 4 Z 1 DSGVO)
- Der Abbau von **Arbeitsplätzen** (z. B. durch Home-Office) sollte als Nicht-Ziel verankert werden.
- keine Reduktion der personellen **Ressourcen** aufgrund der Einführung von MS 365 (z. B. in der IT-Abteilung)
- der Schutz vor einer überschießenden **Überwachung** der Beschäftigten; Verzicht auf die Analyse von Leistungs- oder Verhaltensprofilen oder gar Prognosen. Leistungs- und Verhaltenskontrollen seitens Vorgesetzter oder der IT-Abteilung sollten dabei so weit als möglich vermieden werden. Insbesondere grafische Anzeigen des Arbeits- bzw. Erledigungsstand der KollegInnen (z. B. in Teams [S. 34]) dürfen nicht dazu herangezogen werden, Leistung und Verhalten zu kontrollieren oder bestimmte Beschäftigte(-ngruppen) zu diskriminieren. Ein Generalverbot der Leistungs- und Verhaltenskontrolle mit einem Erlaubnisvorbehalt sollte daher in der BV enthalten sein.

Formulierungsvorschlag für eine BV: MS 365 erzeugt Daten, die zur Kontrolle des Verhaltens und der Leistung geeignet sind. MS 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 ArbeitnehmerInnen 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 wird), wenn sie in einer Betriebsvereinbarung vereinbart wurden (wobei die betreffende Betriebsvereinbarung im Betrieb allen Beschäftigten bekannt gegeben wird) 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.

33 https://mmm.verdi.de/medienwirtschaft/microsoft-und-der-datenschutz-61605

Sollten Auswertungen das **Fehlverhalten** von Beschäftigten aufzeigen, so ist ein einheitliches Vorgehen zu vereinbaren, damit diese Auswertungen nur in Anlassfällen 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 (z. B. Kommunikation, Dokumentenbearbeitung, etc.) ein Mangel der Leistung einer Person oder ein Fehlverhalten einer Person festgestellt, wird seitens der IT-Administration gemeinsam mit dem/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/der Betroffenen liegenden und auch um keinen technisch bedingten Fehler handelt, wird der /die Vorgesetzte und ein Mitglied des Betriebsrates informiert und ein ehestmöglicher Gesprächstermin vereinbart.

Auf Wunsch des Betroffenen kann der Betriebsrat zu dem darauffolgenden Gespräch hinzugezogen werden. Ziel des Gesprächs ist es, zukünftiges Fehlverhalten zu vermeiden (z. B. indem standardisierte Prozesse abgeändert, Löschregelungen modifiziert, Schulungen angeboten, Verhaltensweisen unterlassen werden). 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 wieder holen.

Erst im Anschluss daran, dürfen disziplinäre Maßnahmen unter Einbeziehung des Betriebsrates gemäß § 102 ArbVG (z. B. Verwarnung) 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/Die ArbeitgeberIn verpflichtet sich (und alle allfällig beteiligten Stellen wie den betrieblichen Datenschutzbeauftragten, 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.

Zu jeder in Betrieb befindlichen Anwendung sollte unbedingt eine **Schulung** angeboten werden – vor allem in der ersten Einführungsphase sind LernbegleiterInnen/ExpertInnen für die Beschäftigten von großem Nutzen und sollten daher in der BV festgelegt werden.

Bei den Schulungen ist es einerseits sinnvoll, die direkte Anwendung und die vielfältigen Möglichkeiten von MS 365 zu erlernen, andererseits sollten auch datenschutzrelevante Inhalte in die Schulungen mit einfließen (z. B. wie Datentransfers unterbunden werden können, indem in den persönlichen Einstellungen „optionale Erfahrungen" deaktiviert werden oder wie Daten klassifiziert und damit besonders geschützt werden).

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 Schulungskosten trägt der/die ArbeitgeberIn. 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.

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 freigeschaltet werden und die alten Systeme nicht von einem Tag auf den anderen abgedreht werden.

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

Betriebsräte von Deutschen Medienunternehmen (z. B. RBB, NDR, SWR) haben sich bei der Einführung von Office 365 eingemischt und damit den Prozess maßgeblich beeinflusst. So konnte ein Testbetrieb vereinbart werden. Mit dem Datenschutzbeauftragten wurde zusammengearbeitet. Die Betriebsratsgremien haben sich untereinander koordiniert. Die Klassifikation von Dokumenten wurde vom Betriebsrat mitgestaltet. Schulungen wurde mit Präsenz, also in Anwesenheit von Vortragenden, ergänzend zu E-learning eingefordert. Und ver.di hat diese Erfahrungen zusammengetragen, in „Menschen Machen Medien" im Oktober 2019 veröffentlicht[34] und somit auch anderen Betriebsräten zur Verfügung gestellt.

Da MS 365 (fast) immer auch ein Kommunikationstool ist (besonders bei Outlook [S. 32], Teams [S. 34], SharePoint [S. 42] oder Yammer [S. 48]), jederzeit und von überall erreichbar ist und zahlreiche unterschiedliche und nützliche Anwendungen bereitstellt, fordert es ein extensives Arbeiten geradezu heraus. E-Mails werden nicht selten vor offiziellem Arbeitsbeginn gelesen, Dokumente nach Arbeitsende bearbeitet. MS bietet mehrere Kanäle an, über die kommuniziert werden kann (z. B. Teams [S. 34], Skype [S. 48], Yammer [S. 48]). Das kann, insbesondere bei der Einführung, wenn die verschiedenen Möglichkeiten noch nicht so 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. ArbeitnehmerInnen sind nicht dazu verpflichtet außerhalb der Arbeitszeit Mitteilungen zu erhalten, zu lesen oder zu bearbeiten.

In einer anderen BV heißt es: Die Kommunikations-Kanäle sind auf Teams [S. 34] und Yammer [S. 48] begrenzt.

34 https://mmm.verdi.de/medienwirtschaft/microsoft-und-der-datenschutz-61605 ; 09.12.2020

Idealer Weise stehen auch nach der Ausrollung und Einschulungsphase **AnsprechpartnerInnen** zur Verfügung, die jederzeit auftretende Fragen beantworten können. MS 365 ist ein sehr flexibles und schnelllebiges Programm, das daher auch einer anpassungsfähigen und raschen Auskunftsstelle bedarf. Für Fragen aus der Belegschaft betreffend MS 365 braucht (meist) auch der Betriebsrat eine/n solche/n AnsprechpartnerIn. Diese wäre auch hilfreich, falls der BR Änderungsbedarf an der BV sieht. Eine solche spontan und bedarfsorientiert vorhandene Person könnte auch in die BV aufgenommen werden.

Auf vielen MS Anwendungen können die NutzerInnen eigene Profile anlegen (z. B. MS-Teams [S. 34], Sharepoint, Skype [S. 48] for Business ...). 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.

Aktualisierungen/Updates werden regelmäßig von Microsoft geliefert. Nicht immer gelingt es, einen Überblick über sämtlich Änderungen von MS-Produkten zu behalten – geschweige denn, die Updates vorab einer Prüfung zu unterziehen. Daher empfiehlt es sich, Updates vorab nur für eine Testgruppe in einem geschützten Bereich verfügbar zu machen („Sandkistenanalyse") und erst in einem zweiten Schritt für alle NutzerInnen im Betrieb bereitzustellen.

In der „Microsoft Roadmap"[35] werden Releases vorab angekündigt und man kann sich eine kurze Beschreibung ansehen. Eine Liste der durchgeführten Updates wird wöchentlich im Blog von MS „Office 365 Weekly Digest"[36] veröffentlicht. Um auf dem Laufenden zu bleiben, regt die Gewerkschaft GPA ein Abonnement zumindest einer der beiden Seiten an.

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.

- Updates vor Freigabe im gesamten Betrieb testen (z. B. in einer separaten Testumgebung) und die Testergebnisse mit dem BR besprechen
  - 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 [S. 34])?
  - Hat das Update Auswirkungen auf die Qualifizierung der Beschäftigten (z. B. Trainingserfordernisse)?
  - Sind die Einstellungen im Admin-Center (insbesondere die Deaktivierung von Delve [S. 37]) nach dem letzten Update noch so wie sie es zuvor waren?

- Statt „targeted Release", bei dem Updates zum frühestmöglichen Zeitpunkt durchgeführt werden, sollte „Standard Release" für Updates eingestellt sein; eventuell BR oder IT als „targeted release" einrichten um vorab zu testen, was es Neues gibt

35 https://www.microsoft.com/de-de/microsoft-365/roadmap?market=de&filters; 09.12.2020
36 https://office365weekly.blog/ ; 09.12.2020

Einmal jährlich sollte man sich unbedingt die Mühe machen, das System zu **evaluieren**, um zu überprüfen, ob die Bestimmungen der BV eingehalten werden, die Einstellungen noch aktuell sind, und/oder neue Anwendungen 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 geändert?
- Sind die Auswirkungen auf die Beschäftigten im Bereich der Privatsphäre oder der Menschenwürde, der Überwachung und der Steuerung zu intensiv?
- Ist es zu Problemen gekommen? Können (neue) Einstellungen abgeändert werden? Sollten bestimmte Erweiterungen/Funktionen abgeschaltet werden?
- Muss die BV adaptiert werden?

MS 365 ist ein komplexes, sich stets veränderndes System. Mitunter braucht es Vorkehrungen, damit die Beschäftigten nicht übermäßig überwacht, permanent analysiert und (fremd-)gesteuert werden. Um beurteilen zu können, welche Maßnahmen die Privatsphäre und die Menschenwürde der Beschäftigten schützen, ist das **S-T-O-P-**Verfahren sehr gut geeignet. Man geht dabei entlang einer abgestuften Liste vor, wobei die nächste Stufe erst betreten wird, wenn die vorangehende erfolglos blieb (sogenannte „**Maßnahmenverdichtung**“).

1. **S**ubstituierende Handlung: Bei einer solchen Maßnahme wird eine bestehende Einstellung durch eine weniger belastende ersetzt (z.B. eine unnötige Auswertung wird beseitigt, ein nicht-erforderliches Update wird abgestellt, etc.). Zugegebener Maßen bietet MS dafür wenig Gelegenheit, aber die vorhandenen sollten zumindest genutzt werden.

2. **T**echnische Handlung: dabei wird ein ungewünschter Zustand durch eine technisch-maschinelle Maßnahme beseitigt (z. B. eine problematische Auswertung wird anonymisiert, KollegInnen sehen nicht mehr automatisch wer gerade auf Urlaub ist, sondern erhalten nur dann eine Abwesenheitsnotiz, wenn sie ein E-Mail an eineN *bestimmte* KollegIn schreiben). Auch hier ist der Spielraum den MS 365 zulässt eher gering, dennoch sollte jede Gelegenheit dazu genutzt werden.

3. **O**rganisatorische Handlung: Sollte eine Verbesserung auf technischer Ebene nicht möglich sein, sind organisatorische Vorgaben das Mittel der Wahl (z. B. eine Arbeitsanweisung, die festlegt, dass problematische Systemkomponenten nicht verwendet werden dürfen). Hier wird der wichtigste Ansatzpunkt für die Verhandlung der BV liegen.

4. **P**ersönliche Handlung: 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.

Eine eigene, möglichst fixe „**Microsoft-365-Datenschutzgruppe**“, die aus Beschäftigten unterschiedlicher Bereiche sowie FachexpertInnen besteht (z. B. IT, HR, Recht, Produktion, Geschäftsführung, BR, betriebliche/r Datenschutzbeauftragte/r, externe/r Sachverständige/r) und die sich regelmäßig der Fragen in Zusammenhang mit MS 365 annimmt, ist eine hilfreiche Sache. Manche Betriebe nennen eine derartige Gruppe auch „gemeinsamer MS 365-Ausschuss“. 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).

Die regelmäßige Evaluierung von MS 365 könnte auch zu den Aufgaben einer solchen Gruppe zählen. Mit oder ohne MS-Gruppe, eine Evaluierung sollte jedenfalls stattfinden. MS 365 wird beständig erweitert und abgeändert. Vom Gedanken einer „für die Ewigkeit" abgeschlossenen BV muss man sich bei MS 365-Produkten verabschieden. Dieser Wandelbarkeit wird am besten Rechnung getragen, indem regelmäßig evaluiert und die BV bei Bedarf angepasst wird.

Die vielfältigen Kommunikationskanäle, die vielfältigen – mitunter versteckten – Überwachungsmöglichkeiten und die vielfältigen Verknüpfungen bei MS 365 sind durchaus geeignet, psychische und physische Schäden hervorzurufen und bieten somit Ansatzpunkte für eine **Arbeitsplatzevaluierung** wie sie das ArbeitnehmerInnenschutzgesetz vorsieht. Um diese Risiken zu minimieren, muss der/die ArbeitgeberIn 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.).

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).

DIE HÄUFIGSTEN ANWENDUNGEN VON MS 365

In den folgenden Kapiteln werden jene Anwendungen von MS 365 skizziert, die in den Beratungen der Gewerkschaft GPA am häufigsten vorkommen. Außerdem sind diejenigen Anwendungen dargestellt, die besonderes Überwachungspotential bergen. MS 365 umfasst wesentlich mehr Programme als in dieser Broschüre angeführt sind, wie die Technische Checkliste [S. 52] oder ein Blick auf die Zusammenstellung von Aaron Dinnage auf Github[37] zeigen – auf deren Darstellung im Detail hier jedoch aus Platzgründen verzichtet wird (s. Grafik).

Zur besseren Lesbarkeit sind in den nachfolgenden Kapiteln wieder Kästchen enthalten, die sowohl Beispiele aus bestehenden (Muster-)Betriebsvereinbarungen beinhalten als auch, am Ende des Kapitels zu den jeweiligen Anwendungen zusammenfassend die wichtigsten Punkte, denen man sich bei der Regelung des Programms in einer Betriebsvereinbarung widmen sollte.

OFFICE (= WORD, EXCEL, POWERPOINT)

Bei Office handelt es sich um die wohl bekannteste Anwendung von MS 365. 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 NutzerInnen geben. Wer hat das Dokument erstellt? Wer hat wann welche Änderungen vorgenommen? Diese und andere Informationen werden in Dokumenten gespeichert und können zur Verhaltensanalyse herangezogen werden. Diese Speicherung erfolgt automatisch und *kann nicht abgedreht werden*. Die „Lebensgeschichte" jedes Dokuments ist mit seinen mindestens einhundert bis zu maximal fünftausend Versionen abrufbar. Darüber hinaus werden die Dokumente, so sie auf Sharepoint [S. 42] oder OneDrive [S. 47] abgelegt werden, in sämtlichen Versionen gespeichert. Zwar lässt sich die Anzahl der gespeicherten Versionen konfigurieren, einhundert ist jedoch das Minimum an Speicherungen. Darüber hinaus schreibt Graph [S. 38] im Hintergrund immer mit und verknüpft die Daten mit denen aus anderen Anwendungen.

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

37 https://github.com/AaronDinnage/Licensing

ÜBERBLICK ÜBER AKTUELL VERFÜGBARE ANWENDUNGEN VON OFFICE 365

Quelle: https://pro.jumpto365.com/@/hexatown.com/PTO365-DE

Diese Datenübermittlung kann nicht abgeschaltet werden, zählt aber auch nicht immer zum „berechtigten Interesse" der KundInnen bzw. der Unternehmen, die Outlook nutzen (siehe Kritikpunkte aus Datenschutzsicht [S. 15]). Dazu sollte es also eine Regelung geben. Telemetriedaten sollten an MS ohne Personenbezug übermittelt werden.

Office übermittelt an Microsoft Telemetriedaten über den Systemzustand und über NutzerInnenaktivitäten. Dies kann technisch nicht ausgeschlossen werden. Es ist jedoch seitens der lokalen SystemadministratorInnen sicherzustellen, dass diese Daten nicht geeignet sind, Aussagen über identifizierbare Personen zu treffen, insbesondere, dass keine Benutzer-ID, Betreffzeilen, Inhaltsdaten etc., in den übermittelten Telemetriedaten enthalten sind.

Es ergibt sich Regelungsbedarf:

- Speicherbegrenzung festlegen (Wie viele Versionen werden abgelegt?)
- Speicherdauer limitieren und interne Löschregeln einführen (zumindest soweit das MS 365 technisch ermöglicht, ansonsten organisatorische Löschregeln vereinbaren)
- Speicherort festlegen (wo werden z. B. gemeinsam zu bearbeitende Dokumente abgelegt? Wo werden besonders schützenswerte Daten (nicht) abgelegt?)
- in Kombination mit einem Berechtigungskonzept (wer hat auf welche Speicherorte Zugriff?)
- Interpretationen zu Arbeitsleistung und Verhalten unterbinden (wer hat um welche Uhrzeit ein Dokument/eine Liste mit welchem Ergebnis bearbeitet? darf nicht zur Ableitung arbeitsrechtlicher Maßnahmen herangezogen werden)

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 NutzerInnen meist selbst wissen, wann sie sich ein gemeinsam bearbeitetes Dokument noch einmal vornehmen müssen und nicht über jeden geänderten „Beistrich" ein E-Mail oder SMS ins Postfach bekommen wollen.

OUTLOOK (= E-MAIL, KALENDER, KONTAKTE, CLUTTER, ...)

Outlook verwaltet Termine, Notizen, Aufgaben, Adress- und Telefonbuch, E-Mail und Postfächer. Diese umfassenden Möglichkeiten, viel Speicherplatz und Vernetzungsmöglichkeiten machen Outlook zu einem häufig eingesetzten Programmpaket.
Beim Verwenden der **E-Mail-Funktion** werden im Hintergrund über Graph [S. 38] umfassend Daten gespeichert. AdministratorInnen sehen, wer wann welche Betreffzeile an wen versendet hat. Diese Standardanzeigen sind immer in Exchange und Advanced Threat Protection (ATP) [S. 43] verfügbar und *können technisch nicht abgeschaltet werden*.

Im Exchange-Server können Regeln erstellt werden, wie mit E-Mails und anderen Outlook-Komponenten umgegangen werden soll. Prinzipiell eine empfehlenswerte Vorgehensweise, um beispielsweise die Speicherdauer zweckmäßig zu gestalten und die „Lebensdauer" von E-Mails, Kalendereinträgen, etc. möglichst kurz zu halten. 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 EmpfängerIn nicht einmal und hat auch keine Chance, diese Weiterleitung zu entdecken. Im Fall von Spam-E-Mails, also unerwünschter Post, ist das eine nützliche Vorgehensweise; bei allen anderen E-Mails ist ein derartiges Vorgehen absolut untragbar. Es ist technisch nicht möglich, eine automatische E-Mail-Weiterleitung zu verhindern – bleibt folglich nur ein Verbot derselben per BV oder das „Prinzip Hoffnung", das niemand von den SystemadministratorInnen auf eine solche Idee kommt.
Über den Exchange-Server kann eine Regelung eingerichtet werden, damit sich Sicherungskopien nicht abändern oder löschen lassen – wiederum ohne, dass die NutzerInnen davon in Kenntnis gesetzt werden. Über Graph [S. 38] werden außerdem Verbindungzeiten, Kontakthäufigkeit, Antwortschnelligkeit, etc. ermittelt.
Ebenso problematisch ist im E-Mail-Account die Einstellung „clutter". Ist sie aktiviert, werden „selbstlernend" Prioritäten für E-Mails erstellt. Dabei ordnet MS selbständig, was für die NutzerInnen wichtig ist und was nicht. Anhand der von den NutzerInnen selbst getätigten Kategorisierungen der E-Mails (z. B. wichtig/zur Nachverfolgung/erledigt) lernt MS nach und nach, welche AbsenderInnen schnelle Antworten erfordern, welche erst später Rückmeldung erfordern oder welche Inhalte in der Betreffzeile gar keinen Aufschub erlauben. So sortiert Clutter die E-Mails für die NutzerInnen vor. Dem Arbeiten mit E-Mails wohnt also über unterschiedlichste Verknüpfungen (in Exchange [S. 43], Graph [S. 38], clutter [S. 32],) eine gewisse Verhaltenskontrolle automatisch inne.

Die Gewerkschaft GPA empfiehlt den „Clutter" nicht zu aktivieren und regelmäßig zu überprüfen, ob die Funktion tatsächlich noch *inaktiv* ist.

Um hier Klarheit zu schaffen, die ArbeitnehmerInnen vor unberechtigter Einsichtnahme zu schützen und die SystemadministratorInnen zur Geheimhaltung zu verpflichten, sollte die E-Mail-Kommunikation in der BV geregelt werden:

- **Speicherdauer** (in welchem Umfang werden E-Mails automatisch aufbewahrt? betreffen Aufbewahrungsregeln auch manuell von den NutzerInnen gelöschte E-Mails?)

Von den Beschäftigten gelöschte E-Mails werden für 14 Tage[38] im Papierkorb aufbewahrt und danach unwiederbringlich gelöscht.

- Vertretungsregelungen (Wer darf in das Postfach Einsicht nehmen, wenn jemand plötzlich abwesend ist? Welchen Text sollte die Abwesenheitsnotiz bei geplanten Abwesenheiten enthalten? Wer vertritt eine/n abwesende KollegenIn, wenn E-Mails zu beantworten sind?)

Die für Kommunikationszwecke genutzten Server werden so eingerichtet, dass eingehende Nachrichten generell für persönliche Accounts/Postfächer ausschließlich den vorgesehenen EmpfängerInnen zugestellt werden.

38 Diese Frist ist von MS voreingestellt und kann von Administrator*innen verlängert werden. https://docs.microsoft.com/de-de/exchange/recipients/user-mailboxes/deleted-item-retention-and-recoverable-items-quotas?view=exchserver-2019

Jede/r ArbeitnehmerIn 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.

Die ArbeitnehmerInnen sind aufgefordert, bei vorhersehbaren Abwesenheiten automatische Antworten einzurichten. Bei geplanten Abwesenheiten (Urlaub, Kuraufenthalt) dürfen Weiterleitungen nur von denjenigen vorgenommen werden, auf deren Namen der Account lautet. Sollte dies verabsäumt werden, kann die ernannte Person des Vertrauens auf Aufforderung des/der Vorgesetzten eine solche Abwesenheitsnotiz erstellen.

- **Privatnutzung** festlegen (z. B. eigener Post-Ordner)

Generell ist die Privatnutzung im üblichen Rahmen erlaubt. Dafür steht allen Beschäftigten des Unternehmens ein persönlicher Ordner zur Verfügung. Die ArbeitnehmerInnen sind allerdings angehalten, keine Accounts für die Privatnutzung einzurichten (z. B. Konten bei 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.

- **Verschlüsselung** von E-Mails ermöglichen

E-Mail-Verkehr, der schützenswerte und vertrauliche Daten, insbesondere Gesundheitsdaten enthält, soll immer verschlüsselt versendet werden.

- Die **Einsichtszwecke** von AdministratorInnen eng begrenzen (auf Vermeiden von Schad-Software, Datenangriffe, Viren, Datenabsaugen)
- Stufenweise Kontrollverdichtung[39], wenn AdministratorInnen 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 EmpfängerIn 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. Sollte sich der/die SystemadministratorIn auf den Arbeitsplatz eines/einer MitarbeiterIn aufschalten müssen, so ist dies nur für die Behebung technischer Probleme nach Zustimmung der Betroffenen möglich.

- Falls auf dem Exchange und Advanced Threat Protection (ATP) [S. 43] Einstellungen vorgenommen werden (z. B. Umgang mit Sicherungskopien, automatische Speicherung sämtlicher E-Mails), müssen die Beschäftigten darüber informiert werden

Ein gemeinsamer **Kalender** kann nützlich sein, um Termine abzuklären oder um Bescheid zu wissen, wer wann zur Verfügung steht. Über Exchange [S. 43] kann der Kalender – und dessen Statusanzeigen – für alle (freigehaltenen) NutzerInnen einsehbar gemacht werden. Allerdings dienen Kalender nicht der Arbeitszeit*erfassung*, sondern der Arbeits*organisation*. Kalender sagen also im besten Fall etwas über die Organisationsfähigkeit von KollegInnen aus und sollten folglich auch tunlichst nicht zur Interpretation der Arbeitszeit herangezogen werden, mit der Arbeitszeiterfassung automatisch verlinkt sein oder sonst wie im Zusammenhang mit der Arbeitszeiterfassung abgeglichen werden.
Nachdem im Hintergrund immer Graph [S. 38] mitläuft, könnte ermittelt werden, wann (angeblich) der ideale Termin mit einem/r gewünschten KollegenIn möglich sei, was allerdings auf Parametern beruht, die nicht näher erklärt werden.

39 Siehe dazu Beratungsunterlage der Gewerkschaft GPA

Um die Kalenderfunktion sinnvoll nutzen zu können, wäre es hilfreich in einer BV folgende Punkte zu regeln:

- klare Einsichtsregeln, wer wessen Kalender sehen/verändern kann, Leseberechtigungen und Schreibberechtigungen werden von den einzelnen BenutzerInnen selbstbestimmt vergeben
- klares Vertretungs- und Weiterleitungskonzept sowohl für geplante Abwesenheiten also auch für Notfälle erstellen, wobei die Beschäftigten selbst bestimmen, wer Einsicht in die E-Mails erhält; Vorgesetzte sollten nur in Notfällen die E-Mails der ArbeitnehmerInnen sehen oder an andere weiterleiten (z. B. bei ungeplanten längerfristigen Abwesenheiten, wenn tatsächlich beträchtlicher materieller Schaden für die Firma durch eine Nicht-Einsichtnahme entsteht)
- Einsicht Externer bei Kalendereinträgen unterbinden
- Festlegen, dass der Kalender nicht der Arbeitszeiterfassung und nicht der Dokumentation der Arbeitsaufgaben dient
- Selbstbestimmte und freiwillige Angabe von Präsenz-/Abwesenheitsstatus
- Keine automatisierten Terminvorschläge (via My Analytics/Workplace Analytics [S. 39])
- Keine automatisierte Freigabe des Status
- Die Möglichkeit deaktivieren, andere NutzerInnen über Statusänderungen zu benachrichtigen
- Keine automatisierte Prioritätensetzung (via MS Clutter)
- Keine Standortangaben freischalten
- Auswertungsverbot von Profilen oder eine konkrete Ausnahmeregelung bei anlassbezogenen, begründeten Verdachtsmomenten unter Beteiligung des Betriebsrates
- Keine Vorschläge für Ruhezeiten oder „well-being" (siehe Interpretation von Beschäftigten-Daten durch MS [S. 10])

TEAMS

Teams kann viel; ob Videotelefonie oder gemeinsames Bearbeiten von Dokumenten, ob das Versenden von Nachrichten, die Verknüpfung mit Terminen oder das Chatten mit KollegInnen. Teams ist umfassend zur Zusammenarbeit geeignet, fällt also unter die Rubrik: „Unified Collaboration and Communication" (UCC).

Nachdem Teams in der Cloud betrieben wird, ist es für die ortsunabhängige Kommunikation – insbesondere seit dem Corona-Pandemie-bedingt vermehrten Arbeiten im Home-Office – ein gerne genutztes Instrument. Einfaches Bedienen, 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 – also ohne so genannte „Medienbrüche" – sorgen dafür, dass MS Teams weit verbreitet ist.
Microsoft bietet Teams für bis zu 300 Personen kostenlos an. Bei der Gratis-Version stehen in der Regel Videotelefonie und Chatgruppen für die NutzerInnen im Vordergrund. Die Upload-Kapazitäten (z. B. für die gemeinsame Dokumentenbearbeitung) sind in der Gratis-Variante mit zwei Gigabyte begrenzt. Das Aufzeichnen und Voraus-Planen von Videokonferenzen ist bei der Gratis-Version ebenso wenig möglich wie die sogenannte „Bildschirmfreigabe", bei der während dem Video-Call den anderen TeilnehmerInnen Dokumente oder Präsentationen gezeigt werden können. Weitere Funktionen und Programme von MS 365 stehen erst mit dem Bezahlen von Lizenzgebühren zur Verfügung (z. B. Terminvereinbarungen, Yammer [S. 48], OneDrive [S. 47], etc.).
Teams ist derzeit *die* Anwendung von MS, bei der am meisten Erweiterungen und Verbesserungen programmiert werden, bei der geforscht und massiv Werbung betrieben wird. MS dürfte derzeit viel investieren, um Teams ganz an die Spitze der „Unified Communication and Collaboration (UCC)"-Produkte zu bringen.

„Besitzer" nennt MS diejenigen, die die Berechtigung haben, ein Team zu erstellen, also in der Regel die LeiterInnen. Die Tätigkeiten der letzten sieben bis 28 Tage können mit dem Analysetool für die gesamte Gruppe von diesen „Besitzern/Owner", **ausgewertet** werden. Wie oft tauschen sich die Gruppenmitglieder aus, also wie „aktiv" ist die Gruppe? Wie viele Apps wurden genutzt? Wie viele Megabyte hochgeladen? MS Teams bietet jede Menge Analysemöglichkeiten.

Auch über Verknüpfungen kann die Aktivität in Teams ausgewertet werden. NutzerInnen-Daten aus Teams können in Sharepoint [S. 42] oder OneDrive [S. 47] gespeichert und dort ausgewertet werden. Graph [S. 38] läuft immer im Hintergrund mit und ermöglicht Aus- und Bewertungen. Laut dem Buchautor Kiefer[40] aber *„...brauchen Sie bei der Nutzung des Analyse-Tools keine Bedenken im Hinblick auf den Datenschutz zu haben. Die Auswertungen sind anonym...“* Realistisch ist das nicht, wenn man Teams im Zusammenspiel mit anderen MS Anwendungen betrachtet oder davon ausgeht, dass sich die BenutzerInnen untereinander ohnehin kennen.

Je kleiner die Gruppe desto weniger Anonymität wird gegeben sein. Abgesehen von dieser abgeleiteten Information durch das Wissen um die Zusammensetzung einer Gruppe, ist es GruppenleiterInnen/BesitzerInnen möglich, sich über die Befehlsfunktion „Aktivität“ das Nutzungsverhalten Einzelner anzeigen zu lassen oder sich über die Befehlsfunktion „Organigramm“ zeigen zu lassen, wer mit wem viel oder wenig „Kontakt“ hat. Die Anonymität gegenüber GruppenleiterInnen ist also nicht wirklich gegeben. Daher wird es erforderlich sein, über Bewusstseinsarbeit, Schulungen und BV-Regelungen dafür zu sorgen, dass diese Daten nicht zu unlauteren Zwecken eingesehen und verwendet werden und schon gar nicht zu (nachteiligen) Interpretationen für die Beschäftigten führen.

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 TeilnehmerInnen selbstständig aktiviert und deaktiviert werden.

Sollte MS-Teams in einem Raum verwendet werden, in dem weitere KollegInnen beschäftigt sind, in dem auch betriebsexterne Personen ins Blickfeld einer eingeschalteten Kamera geraten können, müssten diese Personen darüber informiert werden, dass sie im Blickfeld sind. Teams bietet eine Funktion, die den Hintergrund unscharf erscheinen lässt. Diese sollte von den NutzerInnen besonders dann eingeschalten werden, wenn sich andere Personen im Raum befinden (z. B. Mehr-Personen-Büros, Home-Office).

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

MS Teams ermöglicht es, den so genannten „**Status**“ anzuzeigen. Damit können die NutzerInnen einen der von MS vordefinierten Verfügbarkeitsstatus wählen: abwesend, beschäftigt, nicht stören, bin gleich zurück oder verfügbar. Teams gibt automatisch Auskunft darüber, ob die KollegInnen gerade „in einer Besprechung“ oder „in einem Call“ sind, was aufgrund des Terminkalenders oder der aktiven Telefonfunktion festgestellt wird. Diese Präsenz-Information kann auf allen Rechnern und mobilen Geräten angezeigt werden. Der Status wird aber nicht nur in Teams [S. 34] sondern auch in Outlook [S. 32] und Sharepoint [S. 42] angezeigt und im Hintergrund wertet zudem Delve [S. 37] aus, welche Statusangaben die jeweiligen NutzerInnen machen.

Es fragt sich, ob die Angaben im praktischen Arbeitsalltag hilfreich sind (siehe Interpretation von Beschäftigten-Daten – was macht MS 365? [S. 10]) und ob sie von den KollegInnen benötigt werden. Mitunter führen sie zu einem Rechtfertigungsdruck, warum jemand gerade „nicht verfügbar“ ist.

Bei aller Vielfalt und Eloquenz die Teams bietet, kann digitale Kommunikation doch nie die direkte Kommunikation ersetzen. Es sollte daher eindeutig dargelegt werden, wozu Teams verwendet werden soll – und wozu es andere Kommunikationskanäle gibt. Eventuell kann im Unternehmen eine gemeinsame Regelung erarbeiten werden für welche Zwecke Teams genutzt werden soll (z. B. meetings) – und wozu nicht (z. B. das jährliche MitarbeiterInnengespräch). Jedenfalls sollte sich in einer BV widerspiegeln, dass es unterschiedliche Kommunikationsmittel gibt, die jeweils für bestimmte Zwecke geeignet sind (z. B. ist es nicht zweckmäßig die

40 Kiefer, Philip (2020): Microsoft Teams. Effizient im Team organisieren und arbeiten. S. 213; Verlag Markt + Technik

MitarbeiterInnengespräche via Teams zu führen und schon gar nicht dort zu speichern, da so kaum Vertraulichkeit gewährleistet werden könnte).

Für Teams sollten also einige Regelungen in einer BV getroffen werden:

- Eingeschränkte Zweckbestimmung (z. B. interne Kommunikation)
- Ausführliche Schulung
- Ansprechperson bei technischen und organisatorischen Problemen
- Gesichtserkennung als Standardeinstellung deaktiviert (Achtung bei der Aufnahme von Gesichtern handelt es sich um biometrische Daten und diese unterliegen einer besonderen Schutzwürdigkeit und benötigen also eine Einwilligung der Betroffenen)
- **Freiwilligkeit** von Ton- und Bildaufnahmen sowie enge Zweckbindung (z. B. Schulungen, Vorlage für die schriftliche Protokollerstellung); den Hintergrund verschwimmend schalten
- **Mithören/Aufschalten deaktiviert** als Standardeinstellung; auch AdministratorInnen-Rechte so einschränken, dass diese keine Aufzeichnungen durchführen können oder nur für sehr einschränkte Zwecke (z. B. Schulung)

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 TeilnehmerInnen automatisch ausgeschaltet. Bei aktivierter Kamerafunktion ist die Kamera so auszurichten, dass andere Personen nicht dauerhaft vom Sichtfeld der Kamera erfasst werden. Der/die TeilnehmerIn ist verpflichtet, im Raum anwesende Personen über die aktivierte Kamerafunktion zu informieren. Weisungen zur Verwendung des Live-Bildes sind unzulässig.

- Freiwilligkeit von Statusanzeigen sowie Begrenzung der verwendeten Statusangaben (z. B. online/offline); keine Auswertung der vorhandenen Statusanzeigen

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

- Freiwilligkeit der Anzeige zu un-/gelesenen Nachrichten (kann bei den Datenschutzeinstellungen deaktiviert werden)
- Aktuelle, unmittelbare Informationen aller Teams-Mitglieder zu allfälligen Ton- und Bildaufzeichnungen inkl. Widerspruchsrecht

Audio- und Videoinhalte können nach vorheriger Information und ausdrücklicher Zustimmung der TeilnehmerInnen der Konferenz durch den/die OrganisatorIn aufgezeichnet werden. Die Aufzeichnung wird jedem/r TeilnehmerIn auf dem Bildschirm signalisiert. Eine Aufzeichnung sowie deren Weitergabe oder Bekanntmachung an Dritte außerhalb der teilnehmenden Personen, bedarf der vorherigen ausdrücklichen Zustimmung sämtlicher GesprächspartnerInnen. Falls eine Freisprechfunktion genutzt wird, ist der/die TeilnehmerIn ebenfalls zur Information der im Raum Anwesenden verpflichtet.
Zweck der Aufzeichnung von Konferenzen ist die spätere Nachvollziehbarkeit der Konferenz für TeilnehmerInnen und zu Unterrichtende (z. B.: bei Webinaren). Unter einer Aufzeichnung sind auch Chat-Verläufe zu verstehen. Abgesehen von der Aufzeichnung von Webinar-Inhalten sind Weisungen zu einer verpflichtenden Audio- oder Videoaufnahme unzulässig.

- Der TeilnehmerInnenkreis einer Dokumentenfreigabe oder einer Konferenz sollte zu jedem Zeitpunkt für jede/n TeilnehmerIn ersichtlich sein

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

- Anzeigen des Arbeits- bzw. Erledigungsstands der KollegInnen dienen nicht der Leistungs- und/oder Verhaltenskontrolle
- Keine automatisierte Freigabe des Status
- Deaktivierung der Möglichkeit, andere NutzerInnen über Statusänderungen zu benachrichtigen
- Keine automatisierte Prioritätensetzung (via MS Clutter)
- Keine Standortangaben freischalten
- Auswertungsverbot von Profilen; Verbot von Einsicht für Teammitglieder und TeamleiterInnen in Analysen, deren Zweck es ist individuelles Verhalten zu vergleichen oder zu beurteilen

Das Unternehmen sichert zu, dass keine personenbezogenen Auswertungen eingesehen werden und keine Überwachung von Leistung oder Verhalten mittels MS Teams personenbezogen eingesehen wird. Eine Auswertung und Analyse von personenbezogenen Daten für Profiling gem Artikel 4 Z 4 DSGVO (insbesondere zur Leistungsbeurteilung), ist jedenfalls untersagt.

DELVE

Delve ist seit 2015 ein fixer Bestandteil von MS 365. Delve sammelt Daten aus sämtlichen Anwendungen und stellt sie wiederum für andere Anwendungen grafisch dar. Delve ist die Schnittstelle zwischen den verschiedenen Verwendungen und somit essentiell für die technische „Verständigung" der MS 365-Anwendungen untereinander.
MS bezeichnet Delve als „Dokumentenmanagementsystem". Es bietet als einziges Tool in MS 365 einen Überblick über sämtliche Aktivitäten unabhängig davon über welche Apps und Anwendungen sie laufen – vorausgesetzt sie finden in MS 365 Anwendungen statt – und ist daher gut als Suchfunktion geeignet (z. B. nach Stichwörtern quer über alle Laufwerke, E-Mails, Fotos und Protokolle verteilt). Delve sammelt zusammengefasste Daten wie die Anzahl der NutzerInnen, Anzahl der LeserInnen und die Kommunikationshäufigkeit untereinander.
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 BearbeiterInnen? 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 NutzerInnen nicht ersichtlich. Offengelegt ist, dass folgende Parameter einfließen: das persönliche Kommunikationsverhalten, die Häufigkeit von (gemeinsamen) Dokumentenaufrufen und -bearbeitungen (z. B. Excel) sowie Terminkalender und Notizen. Delve bietet NutzerInnen die für ihre jeweiligen Arbeitsaufgaben „passenden" Dokumente und Informationen automatisch an. Darin kann auch ein selbst definiertes „Board" angelegt werden, wo die Informationen, die man selbst für interessant hält, als Favoriten dargestellt werden. Delve kann zwar technisch abgeschaltet werden, erfasst werden NutzerInnendaten aber dennoch über Graph [S. 38]. Durch das Deaktivieren von Delve ist die Aktivität anderer NutzerInnen nicht mehr *ersichtlich* und andere NutzerInnen sehen die eigene Aktivität ebenso wenig.
Auch SystemadministratorInnen können bei Delve nur begrenzt technische Einstellungen vornehmen. Beispielsweise können die bis zu 90-tägigen Löschfristen[41]

41 Bei der Datenschutzfolgenabschätzung der Niederländischen Datenschutz Behörde bzgl. der Programmversion Office Pro wurde eine Minimum-Speicherdauer von 30 Tagen und eine maximale Speicherdauer von 18 Monaten für „event Logs" auf US-amerikanischen Servern festgestellt. (https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2018/11/07/data-protection-impact-assessment-op-microsoft-office/DPIA+Microsoft+Office+2016+and+365+-+20191105.pdf ; 10.12.2020)

mancher Protokolle nicht geändert werden, das Teilen von Dokumenten mit anderen NutzerInnen („sharing") kann teilweise nicht deaktiviert werden. Daher müssen organisatorische Maßnahmen getroffen werden, um übermäßige Kontrollen der Beschäftigten über Delve zu unterbinden (siehe dazu auch das STOP-Prinzip in Allgemeine Gestaltungsvorschläge: [S. 28]).

Es ist daher ratsam in der BV zu regeln:

- Für welche Zwecke Daten ausgewertet werden dürfen (z. B. Suche nach verlorenen Unterlagen)
- Wer worauf Zugriff erhalten soll, z. B. Zugriff nur unter strengem Reglement gestalten (z. B. im Beisein des Betriebsrates) oder Zugriff nur auf eigenes Board erlauben und keinesfalls die Freigabe für die Boards anderer KollegInnen!
- Information der Beschäftigten über die Funktionen von Delve – auch wenn MS hierzu nicht sehr transparent ist, so sollte es zumindest seitens des Arbeitgebers/der Arbeitgeberin so weit als möglich versucht werden
- Freiwilligkeit der Verwendung von Delve vereinbaren
- Ranglisten/Personen-Scoring/Personenvergleiche ausschließen
- ODER: Delve deaktivieren – und immer wieder nachprüfen, ob die Einstellung im Admin-Center auch aktuell ist

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

- ODER: Delve nur für eine möglichst kleine Gruppe von AdministratorInnen aktivieren und mit diesen eine Geheimhaltungserklärung vereinbaren

Eine Möglichkeit, *ohne* Delve zu arbeiten wäre es, MS365 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 ohne Cloud-Services arbeiten.
Die eigentlichen Vorteile von MS 365 (z. B. erleichterte Kooperation, Übersichtlichkeit, einfache Anwendung, geringer lokaler Speicher-Ressourcenverbrauch, Zeit- und Ortsunabhängigkeit, Kompatibilität mit zahlreichen andere Anwendungen) gehen damit allerdings auch verloren und es würde sich die Frage stellen: warum nicht gleich ein vertrautes, bewährtes und idealer Weise schon mit einer Betriebsvereinbarung geklärtes System verwenden?

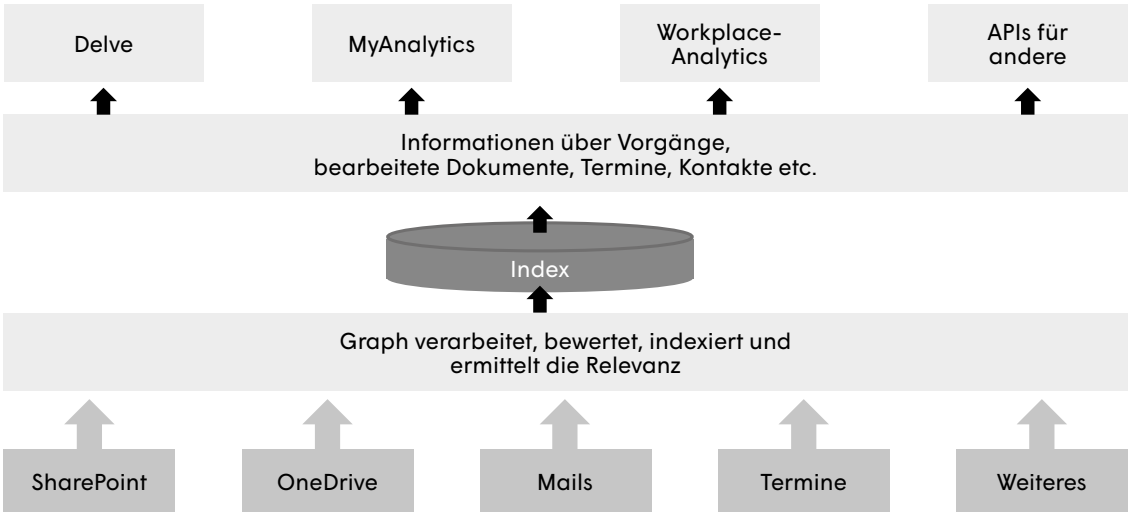
GRAPH

Über Graph (s. Grafik) werden NutzerInnen-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 und stellt sie anderen MS-Anwendungen zur Verfügung.[42]

Graph bewertet die Aktivitäten sämtlicher NutzerInnen und bildet einen Index der angeben soll, welche NutzerInnen, welche Anwendungen, welche Dokumente „relevant" sind. Graph gibt Empfehlungen zu Dokumenten, Kontakten, Ereignissen oder auch Kommunikationen ab. Auf welchem Weg Graph diesen Index erstellt und welche Berechnungen dahinter ablaufen, wird von MS nicht preisgegeben. Die Information von MS beschränkt sich weitgehend darauf, dass „Künstliche Intelligenz" zum Einsatz kommt. Graph ist ein sogenanntes „selbstlernendes System." Das bedeutet, dass NutzerInnen mit jeder Aktivität in MS 365 bekanntgeben, was sie tun – und lassen – und diese Informationen dazu dienen, Vorlieben zu berechnen.
Diese permanente Leistungserfassung läuft immer im Hintergrund mit. Zwar kann man verhindern, dass die Auswertungen angezeigt werden (z. B. indem man Delve [S. 37] oder My Analytics/Workplace Analytics [S. 39] deaktiviert), doch legt MS nicht transparent dar, was Graph genau macht. Außerdem wurde festgestellt, dass Auswertungen auch jene Daten beinhalten, die

42 Wer SAP kennt fühlt sich nicht zu Unrecht an das „Data-Warehouse" erinnert. Allgemein wird eine solche Funktion meist als „Data-Mining" bezeichnet.

FUNKTION VON GRAPH



während dem „inaktiv" setzen von Delve erzeugt wurden. So wurden z. B. Termine mit viel E-Mail-Verkehr als „unfokussiert" gewertet, obwohl My Analytics/Workplace Analytics [S. 39] am Tag des Termins eigentlich deaktiviert war. Daher liegt die Vermutung nahe, dass Graph trotz Abschalten weiter im Hintergrund personenbezogene Daten sammelt. Man verhindert mit dem Abschalten also nicht, dass die Daten der NutzerInnen von MS verarbeitet werden. Technische Verhaltenskontrolle wohnt dem System von MS 365 per se inne.

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

SystemadministratorInnen könnten, auch wenn NutzerInnen es nicht aktiv verwenden, das so genannte „Benutzeraktivitätsberichtsprotokoll" (z. B. in OneDrive [S. 47]) 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 (siehe auch BV-Formulierungsvorschlag Allgemeingültige Gestaltungsvorschläge – wie sollte MS 365 geregelt werden? [S. 23]).

- Privacy-Einstellungen so vornehmen, dass möglichst viele Daten in anderen MS 365-Anwendungen verborgen werden, also nicht in die Graph-Analyse einfließen
- Allfällig vorhandene Schnittstellen (API) 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
- Das Erstellen eigener, zusätzlicher Auswertungen (scripts) seitens der AdministratorInnen unterbinden

MY ANALYTICS/WORKPLACE ANALYTICS

Die beiden Analyse-Tools dienen laut Eigendefinition von MS dazu, Gewohnheiten der NutzerInnen zu erkennen. Sie sollen durch die Analyse ebendieser Gewohnheiten und persönlichen Arbeitsweisen helfen, „noch produktiver" zu arbeiten. „*Werden Sie noch produktiver*" regt MS auf seiner Website die NutzerInnen an „*indem Sie Ihre Arbeitsmuster mit MyAnalytics in vier Kernbereichen auswerten: Fokus, Wohlbefinden, Netzwerk und Zusammenarbeit.*"
Beide Analytics-Tools greifen auf Daten aus Graph [S. 38] zurück , wobei sie vorwiegend Daten aus Outlook; E-Mails , Kalender, Kontakte [S. 32], etc. verwenden, um das NutzerInnenverhalten zu analysieren und „mitzulernen".

In My Analytics wird das *eigene* Verhalten analysiert (z. B. Wieviel Zeit war man mit bestimmten KollegInnen in Meetings? Wie oft hatte man mit dem/der ChefIn Kontakt? Wie schnell hat man E-Mails durchschnittlich gelesen?

Wurden die von einem selbst verschickten E-Mails gelesen, respektive beantwortet? Welche Aufgaben wurden erledigt? etc.) und man erhält Tipps (z. B. gegen Entgrenzung, Vorschläge für „Fokuszeiten[43]", KollegInnen mit denen man Kontakt aufnehmen sollte, welche E-Mails bevorzugt behandelt werden sollten). In einem E-Mail-Newsletter erhält jede/r NutzerIn auf das persönliche Verhalten abgestimmte Vorschläge, wie das eigene Verhalten effizienter gestaltet werden kann. MS schreibt dazu auf seiner Website: „*Get tips on how to plan your calendar, spend less time in low-quality meetings, and write more effective E-Mails*."

My Analytics ist nur für den/die NutzerIn selbst einsehbar. Vorgesetzte bekommen die Auswertungen nicht automatisch zu sehen. Die AdministratorInnen können die Anwendung auch nicht freigeben.
Sieht man die Empfehlungen von MyAnalytics, erhält man Einblick, wie Graph [S. 38] arbeitet, welche Schlüsse gezogen werden und stellt fest, dass die Hinweise eher wenig aussagen (siehe auch: Interpretation von Beschäftigten-Daten durch MS – was macht MS 365? [S. 11]). Ein Nutzer von MyAnalytics hat seine Erfahrungen so beschrieben: „*Die Informationen, die MyAnalytics liefert, sind allerdings von überschaubarer Qualität und überschaubarem Nutzen. Im günstigsten Fall ist MyAnalytics Zeitverschwendung*."[44]

Im schlechtesten Fall, wenn die Analysen nicht nur für Einzelne, sondern für Gruppen oder Abteilungen zur Verfügung gestellt und miteinander abgeglichen werden, entstehen durch derartige Netzwerkanalysen auch Bewertungen (z. B. wer arbeitet produktiver/engagierter/effizienter als andere?)[45], die wiederum das soziale Leben im Betrieb nachhaltig beeinflussen können.
Auf Workplace Analytics werden die Daten des gesamten Teams bzw. der gesamten Abteilung oder der gesamten Belegschaft für Führungskräfte im Vergleich mit der „Produktivität" anderer dargestellt (z. B. Anzahl der Termine, der erledigten Tasks, beantworteten E-Mails, etc.). Im Dashboard von Workplace Analytics kann die Beziehung zwischen Teams mit unterschiedlich starken Linien dargestellt und nach Kommunikationswegen gefiltert werden (z. B. E-Mail, Chat, Meeting). So könnte eine Darstellung ergeben, dass Team A mit Team B insgesamt betrachtet eng kooperiert, sich aber noch nie in einem Meeting persönlich getroffen hat.
Workplace Analytics wurde in einer ersten Variante 2015 unter dem Namen „Delve Organisational Analytics" auf den Markt gebracht und 2017 für Firmenkunden dem MS 365-Paket hinzugefügt.[46] Derzeit ist ein Abonnement, also eine Lizenz, auf dem europäischen Markt nicht erhältlich. Sollte ein amerikanischer Konzern(-teil) allerdings Analytics gekauft und eingeschalten haben, wird es wohl auch in den Niederlassungen in Europa verfügbar sein.

Ein Bericht auf Heise[47] über dieses Tool wurde auf Twitter[48] aufgegriffen und hat im November 2020 große Wellen bis über den Atlantik geschlagen (siehe Kritikpunkte aus Datenschutzsicht im Überblick [S. 12]). Dass hier ArbeitnehmerInnen-Überwachung im großen Stil praktiziert wird, wurde öffentlich beim Namen genannt und hat zu zahlreichen – internationalen – Reaktionen geführt.

Workplace Analytics arbeitet zwar mit pseudonymisierten Daten. Allerdings gibt MS selbst zu, dass das Risiko der Identifizierung dennoch besteht. Mittels WorkplaceAnalytics könnten Vorgesetzte sich anzeigen lassen, wer mit wem wann Dokumente bearbeitet hat, Termine vereinbart hat, wer wessen E-Mails besonders rasch bearbeitet, wer mit wem wann gechattet hat, etc. Auf diese Art möchte MS 365 Informationen bereitstellen zu „Quellen für Zeitverlust, (...) Stressindikatoren, (...) Aussagen zu Stimmung und dem Engagement der Belegschaft.[49]" Und letztendlich „die Produktivität von Wissensarbeitern messbar machen" mit der Ankündigung „die besten, die produktivsten und die zufriedensten Arbeitnehmer bestimmen zu können[50] (zum Sinn und Unsinn mancher Statistiken von MS siehe Interpretation von Beschäftigten-Daten durch MS [S. 11]).[51]

---

43 Die Funktion „Fokus" plant ein bis zwei Stunden pro Tag ein, an denen ohne „Störung" durch Meetings (z. B. von MS Teams) gearbeitet werden kann.
44 Jes-Seminar im September 2020.
45 Zu den verschiedenen Möglichkeiten der innerbetrieblichen Analyse sozialer Netzwerke, wurde von der deutschen Hans Böcker Stiftung 2018 eine spannende Publikation geschrieben: Heinz-Peter Höller, Peter Wedde: Die Vermessung der Belegschaft, Mining the Enterprise Social Graph https://www.boeckler.de/pdf/p_mbf_praxis_2018_010.pdf
46 https://www.silicon.de/41652823/microsoft-ergaenzt-office-365-um-workplace-analytics
47 https://www.heise.de/news/Anwenderueberwachung-durch-Microsofts-Office-Software-4968615.html
48 https://twitter.com/WolfieChristl/status/1331221942850949121 ; 22.12.2020
49 https://www.heise.de/news/Anwenderueberwachung-durch-Microsofts-Office-Software-4968615.html ; 10.12.2020
50 Höller 2018: 31
51 Das holländische Justizministerium schreibt in seiner Datenschutzfolgenabschätzung: "Workplace Analytics and the Activity Reports in the Microsoft 365 admin center provide very detailed insights in the behaviour of groups of employees. Although Microsoft aims to provide pseudonymised insights relating to five people or more, Microsoft also warns that individual employees may still be identifiable (such as the director)." https://www.lawinsider.com/documents/7IgiwHRzs7k

Es spricht viel dafür, weder MyAnalytics noch WorkplaceAnalytics zu kaufen bzw. zu aktivieren! (Workplace müsste ohnehin zusätzlich lizensiert werden und ist 2020 noch nicht auf dem Europäischen Markt erhältlich.).
Den Zugriff auf Delve [S. 37] sollte man jedenfalls für alle NutzerInnen sperren (über Sharepoint [S. 42]).

Falls sich Analytics nicht unterbinden lässt, sind folgende Verwendungsverbote in der BV festzuhalten:

- grundsätzlicher Verzicht der Nutzung personen- und kleingruppenbezogener Analysefunktionen, sodass ausschließlich Personengruppen, die mehr als zehn Individuen erfassen, zusammen dargestellt werden
- auf Analyse der Nutzungsintensität verzichten
- Maßnahmen, die auf Auswertungen von Analytics basieren, für unwirksam erklären

Maßnahmen, die auf unzulässig durchgeführten Verhaltens- oder Leistungskontrollen oder unzulässig verarbeiteten personenbezogenen Daten beruhen oder aus ihnen resultieren, sind unwirksam und müssen zurückgenommen werden.

- Falls das Unternehmen Schnittstellen zu externen Programmen verwendet, müssen diese unbedingt von der Verwendung der Daten ausgeschlossen werden; somit können keine Daten aus Graph über den Umweg über andere Programme oder Drittanbieter verwendet werden.
- Updates vorab prüfen (siehe Allgemeine Gestaltung – wie sollte MS 365 geregelt werden? [S. 22])

STREAM

Auf diesem Videoportal können firmenintern Videos hochgeladen werden. Informationen werden mit Hilfe kurzer Videos unter den Beschäftigten verbreitet. Stream wird für Team-interne Kommunikation und Schulungen eingesetzt.
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
- 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 Anwendung sondern um eine Funktion, die in einigen Anwendungen von MS 365 beinhaltet ist (z. B. Outlook [S. 32], Teams [S. 34]). Über die Anzeige des Status können andere NutzerInnen erkennen, ob jemand gerade erreichbar ist oder auch *warum* jemand nicht erreichbar ist.
Diese Information ist nicht nur für die KollegInnen ersichtlich, sondern auch MS stellt damit Berechnungen in Graph [S. 38] an und gibt in My Analytics/Workplace Analytics [S. 39] Tipps, wie die Zeiteinteilung optimiert werden könnte.

Manche Einstellungen bei den Statusanzeigen sind problematisch:

- So schickt beispielsweise „Benachrichtigen wenn verfügbar" eine Nachricht an die Person, die dies anfordert, sobald der/die gewünschte Kollegeln die Statusinformation entsprechend ändert – mit dem kleinen

Schönheitsfehler, dass die gewünschte Person nichts davon weiß und diese Benachrichtigung, auch wenn sie wollte, nicht unterbinden kann. Eine SMS „Bitte ruf mich zurück" wäre ausreichend und würde die Person nicht einer heimlichen Überwachung aussetzen.
– von der Verwendung dieser Funktion sollte Abstand genommen werden.

- Wird der Status manuell zurückgesetzt, wird dennoch automatisch über den Terminkalender ein Status bestimmt – das manuelle Rücksetzen kann man also getrost bleiben lassen.

- Die vier Voreinstellungen können nicht auf selbst definierte, besser passende Status abgeändert werden.

In der BV zu MS 365 sollte geregelt werden:

- freiwillige Nutzung der Statusfunktionen

- eine einzige Statusanzeige für jede Gelegenheit und alle NutzerInnen vereinbaren (z. B. „verfügbar") oder zumindest möglichst wenige Status-Möglichkeiten nutzen (z. B. „abwesend/verfügbar" ist in der Regel ausreichend); allenfalls eine Einstellung für urlaubsbedingte Abwesenheiten vereinbaren

- keine über den gegenwärtigen Zeitpunkt hinausgehenden Informationen auswerten (z. B. ist seit fünf Stunden in einem Meeting, war letzten Monat 90 % nicht verfügbar)

- historische Rückschau der Status-Zeiten (z. B. Verfügbarkeit, Online-Zeit...) unterbinden

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[52]) wird weder vom System vorgenommen, noch ist die Aufzeichnung /längerfristige Beobachtung zulässig.

SHAREPOINT

SharePoint ist ein zentraler Dienst von MS, der quasi als eigener Server zur Verfügung steht. Über SharePoint können beliebig viele und beliebig große Plattformen eingerichtet werden. Äußerlich ähnelt SharePoint einem Blog, auf dem unterschiedlichste Formate eingehängt werden können wie beispielsweise eine Dokumentenbibliothek, ein Telefonverzeichnis, aktuelle Informationen, geteilte Kalender, Postfächer, etc. Je nachdem, was das Unternehmen gerne über SharePoint laufen lassen möchte, ist diese Plattform geeignet, die jeweiligen Erfordernisse bereitzustellen.

Was auf SharePoint gelöscht wurde, bleibt weitere 90 Tage im Papierkorb. Das ist die Werkseinstellung von MS. Sollte man diese Einstellung nicht beibehalten wollen, kann das in Security and Compliance [S. 44] über die „retention library" geändert werden. Dies ist empfehlenswert.

In der BV sollte geklärt werden:

- Eindeutiger Zweck von SharePoint (z. B. gemeinsame Bibliothek und Dokumentenablage) und festlegen, welche Daten nicht über SharePoint abgelegt werden sollen (z. B. mittels einer Daten-Klassifikation, die ausschließt, dass Gesundheitsdaten auf SharePoint liegen)

- Schulungen für AnwenderInnen in denen eigens darauf hingewiesen wird, wie eine Analyse erfolgt und wie sie abgeschaltet werden kann

- Zugriffs- und Änderungsberechtigungen; im Idealfall wird auf der Einstiegsseite dargestellt wer die TeilnehmerInnen sind/wer zum Benutzerkreis zählt und wer Hauptverantwortliche/r/ BesitzerIn/ „Owner" der SharePoint-Seite ist

- BesitzerInnen/Owner sind für die Gestaltung der Seite, für das Rollen- und somit auch Zugriffskonzept ihrer Seiten verantwortlich und müssen für ihre Nachfolge Sorge tragen. Sie erhalten eigene Schulungen.

52 Diese Frist ist von MS festgelegt und lässt sich nicht manuell abändern.

- Als Standardeinstellung ist Delve [S. 37] deaktiviert und kann nur von den NutzerInnen mit deren ausdrücklicher und freiwillig erteilter Zustimmung aktiviert werden; Anzeigen sind in Folge auch ausschließlich den NutzerInnen persönlich zugänglich

- Aufbewahrungsdauer festlegen („retention policy" bzw. maximale Anzahl an Versionen für gemeinsame Dokumente)

- Der Betriebsrat hat Zugriffsrechte auf jede in SharePoint erstellte Seite, um die Einhaltung der BV zu überprüfen

- Allfällige, weitere eingebundene Apps und Schnittstellen müssen dargestellt werden

- Allfällige Synchronisation mit firmeneigenen Servern festlegen (z. B. Häufigkeit, Datenvolumen)

EXCHANGE UND ADVANCED THREAT PROTECTION (ATP)

Über diese Applikation werden E-Mails und Kalender verwaltet. Posteingangsregeln, Weiterleitungen, Spamfilter, Schadensabwehr etc. werden über Exchange eingestellt. Die „Advanced Threat Protection" dient – wie der Name unschwer erkennen lässt, der Schadensabwehr. MS hat dafür „selbstlernende" Systeme programmiert, die im Voraus erkennen sollen, ob, wo und wodurch Gefahrenpotential besteht. Gehackte Anmeldedaten, betrügerische E-Mail Schadsoftware soll hier erkannt und abgewehrt werden.
Bedrohungs-Szenarien werden anhand der vorhandenen Daten entwickelt (z. B. Attachments von Fishingmails werden von den Beschäftigten geöffnet), woraufhin ein Programm entwickelt wird, dass einen Angriff simuliert und über diese „Schulung" zukünftigen Schaden zu vermeiden erlernt. „Sensibilisierung und Training" nennt MS dieses Vorgehen.
Kalender und E-Mails [S. 32] können in Exchange synchronisiert werden und „voneinander lernen". Der Kalender „lernt" beispielsweise, dass während eines Fluges keine E-Mail empfangen werden können, dass bestimmte Besprechungen länger dauern als geplant, etc.
Über die Funktion „Clutter" werden die Kommunikationsgewohnheiten der NutzerInnen analysiert (z. B. Prioritätensetzung, Lese- und Antwortgeschwindigkeit, etc.), um auf dieser Basis weitere Regeln zu erstellen. Das System „lernt".

In der BV müssen die Regeln für Outlook (= E-Mail, Kalender, Kontakte, Clutter,...) [S. 32] und Teams [S. 34] mit denen von Exchange in Einklang stehen.

Außerdem zu regeln ist:

Prozedere bei Trainings/Schulungen/Tests zur Bewusstseinsbildung im Umgang mit Sicherheitslücken
- Information der Beschäftigten,
- Beteiligung des BR,
- Folgen bei nicht-adäquater Reaktion der Beschäftigten auf Sicherheitsbedrohungen (z. B. Nachschulung aber keine personellen Konsequenzen, keine Versetzung, Vorgehen bei mehrmaligem Fehlverhalten innerhalb kurzer Zeit ist mit dem BR abzustimmen, etc.)

eDISCOVERY

Diese Funktion dient dem Wiederauffinden von Texten, die über Outlook [S. 32], Teams [S. 32] oder Yammer [S. 48] ausgetauscht wurden. Für DatenforensikerInnen ist eDiscovery 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 MitarbeiterInnen", womit auch schon offenbart ist, dass es sich zur Überwachung der Beschäftigten bestens eignet.

In den meisten Branchen und Betrieben sind die üblichen Archive und Speicherorte ausreichend, weshalb man den extra Behalte-Bereich eDiscovery im Arbeitsalltag vermutlich nicht braucht. Die Empfehlung lautet, eDiscovery nicht zu aktivieren.

Für die Regelung in einer BV sollte beachtet werden:

- Zugriffsbeschränkungen (z. B. im Anlassfall für ForensikerInnen)

- eingeschränkte Zwecke (z. B. tatsächlich vorliegende Gerichtsprozesse/Gerichtsgutachten, schwerwiegende Sicherheitsattacken)

- Speicherdauer

MS SECURITY AND COMPLIANCE (Z. B. WINDOWS HELLO, THREAT EXPLORER, BITLOCKER)

In „Security & Compliance" werden die Sicherheitsrichtlinien für die anderen MS 365-Programme festgelegt. Die SystemadministratorInnen können hier die Funktionsweise der Sicherheitstools testen, analysieren, kontrollieren oder (strenger) gestalten. Hier wird festgelegt, welche Speicherprozeduren wofür gelten und 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 weitere Tests und Schulungen zu entwickeln. Außerdem werden Benchmarks im Vergleich zum Sicherheitsrisiko anderer Firmen erstellt, forensische Berichte geliefert sowie Empfehlungen zur besseren Sicherheit geschaffen.
Zugriffsmöglichkeiten werden heutzutage 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 mobilen Geräten nennt MS „bitlocker".
„Windows Hello" bietet biometrische Zugriffskontrolle an (z. B. Fingerprint), um eine eindeutige Authentifikation zu ermöglichen. Biometrische Zugriffssperren werden vor allem beim Zugriff zu Cloud-Services von MS genutzt, um NutzerInnen automatisch informieren zu können, sollten ihre Passwörter/PINs im Dark Web verkauft werden.[53]

In einer BV sollte daher auf folgende Themen geachtet werden:

- Zweckbeschränkung auf technische Auswertung und Korrektur von Fehlern oder Zwischenfällen
- Speicherbeschränkung für Protokolle auf 90 Tage
- Zugriffsbeschränkungen (Welche Zugriffe dürfen mit welcher Art von Passwort erfolgen?)
- Rücksprache mit dem Betriebsrat, wenn neue Regeln für Security und Compliance erstellt werden
- Benachteiligungsverbot (z. B., wenn auf Simulationen zu Schulungszwecken falsch reagiert wird)
- Keine Verwendung biometrischer Merkmale (via Hello) für eine Authentifizierung!

AZURE ACTIVE DIRECTORY

Azure ist die Cloud-Plattform von MS auf der alle Anwendungen für alle NutzerInnen zur Verfügung gestellt werden. Darin wird der Zugriff sämtlicher Geräte reguliert. Ohne Azure kann MS 365 nicht in der Cloud genutzt werden. Ohne Azure gäbe es keine BenutzerInnenverwaltung und keine Zugriffsmöglichkeit auf die verschiedenen Anwendungen von MS 365.

Die Benutzerverwaltung über Azure wird von MS bei den Lizenzversionen gratis dazu geliefert.

Im Active Directory melden sich die NutzerInnen an und identifizieren sich, wobei die IP-Adresse ebenso automatisch gespeichert wird, wie der (geschätzte) Standort. 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 Augenscan verwendet werden, ist der Zugang zu den Anwendungen unterschiedlich sicher.

Biometrische Merkmale zu verwenden ist zwar sicher, weil sie nur einem Menschen auf der Welt zugeordnet werden können, 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.[54] Umso überschießender wird es sein, ein solch heikles Merkmal für relativ simple Vorgänge wie beispielsweise das Einloggen in Outlook (= E-Mail, Kalender, Kontakte, Clutter,...) [S. 32] zu verwenden.
Diese Anmeldevorgänge werden aufgezeichnet und somit haben AdministratorInnen die Möglichkeit gewisse Verhaltensmuster abzuleiten (z. B. Wer meldet sich wann an? Von welchem Standort melden sich der/

53 Ob die eigene Mail-Adresse in falsche Hände geraten ist, kann man auf der unabhängigen Plattform „Have I been Pwned" (zu deutsch: „Wurde ich erwischt.") überprüfen. https://haveibeenpwned.com/
54 OGH 9 ObA 109/06d

die NutzerIn 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
- Eindeutige Zwecke, wofür Azure verwendet werden darf
- Verhaltensauswertung auf technische Auswertungszwecke reduzieren, keine Vergleiche, wer sich wann von wo eingeloggt hat
- Allfällige Verwendung privater Geräte und deren Zugang regeln
- Für besonders schützenswerte Daten eine 3-Faktor-Authentifizierung zu verwenden
- Keine biometrische Identifikation

AZURE INFORMATION PROTECTION (AIP)

Sämtliche Informationen werden in 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 Entstehungsgeschichte, Zugriffe, allfällige Weitergabe etc. nachvollzogen. Es soll dadurch herausgefunden werden, ob strafrechtlich relevante Ereignisse stattgefunden haben (z. B. Betrug, Spionage, Insider-Handel aber auch Compliance-Verstöße) bzw. wie sie zustande gekommen sind. Eine Durchleuchtung aller Dokumente, die vornehmlich dem Schutz vor falscher Verwendung dient, kann jedoch bei manchen Daten problematisch werden (z. B. BR-Korrespondenz).
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 (wenn z. B. die AIP „lernt", dass „rote Socken" eine Beleidigung ist und die Packliste eines sozialdemokratischen Festredners als beleidigend einstuft).

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.

In einer Betriebsvereinbarung sollte geregelt sein:

- Datenkategorisierung
- Strenge Zugriffsregelungen
- Klares Prozedere, was im Falle eines Verdacht zu geschehen hat (siehe auch „Stufenweise Kontrollverdichtung" in der Muster-Rahmen-BV und Muster zur Whistleblowing-BV der Gewerkschaft GPA)
- Klare Speicherfristen

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.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

Durch die Analyse typischer Muster von Sicherheitsvorfällen, soll herausgefunden werden, ob ähnliche Vorfälle bevorstehen. In Echtzeit sollen Auffälligkeiten in Logdateien von Betriebssystemen, Datenbanken und Anwendungen präsentiert, analysiert und allfällige Sicherheitslücken behoben werden. Es handelt sich um eine Sicherheits-Anwendung zur Auswertung und Prognose.

- 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, ist die „**stufenweise Kontrollverdichtung**" (siehe Rahmen-Datenschutz-BV der Gewerkschaft GPA) ein probates Mittel.

DATA LOSS PREVENTION

Diese Anwendung findet sich im „Security and Compliance Center" und dient (wie schon der Name ankündigt) dem Auffinden verloren gegangener Daten. Hiermit kann festgestellt werden, ob Daten (illegal) abgegriffen wurden. Die Vorgaben, was als auffällige oder gefährliche Aktivität gilt, werden über Data Loss Prevention erstellt (z. B. Kreditkartennummern dürfen nicht per E-Mail versendet werden). Es kann ein Schwellenwert definiert werden, wann eine Warnung ausgeschickt wird (z. B., wenn Dokumente zu Steuern und Abgaben schon nach vier Jahren statt wie vorgeschrieben nach sieben Jahren gelöscht werden).

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

Die Regelungen sollen jenen in anderen Sicherheitsanwendungen von MS entsprechen (siehe: MS security and Compliance (z. B. windows Hello, Threat Explorer, Bitlocker...)) [S. 44], Security Information and Event Management (SIEM) [S. 46], Azure Information Protection (AIP) [S. 41]) und daher sind auch hier die wichtigsten Punkte:

In einer Betriebsvereinbarung zu regeln sei:

- Zugriff auf IT-Abteilung beschränken
- Regelung und Information an die Beschäftigten was im Falle des Auftauchens eines Sicherheitsrisikos 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

INTUNE

Diese App ist dazu da, Geräte zu verwalten und zu überprüfen. Intune ist eine eigene Cloud-Anwendung innerhalb der sogenannten „MS Enterprise Mobility Suite (EMS)", über die z. B. Virenscans durchgeführt werden können, Fernzugriff und die Sperre von Accounts veranlasst werden können, Geräte geortet werden können, etc.

- Zugriffsmöglichkeiten festlegen und auf IT beschränken
- Die Beschäftigten zu Updates etc. informieren
- Achtung beim Einbinden von privaten Geräten, davon ist eher abzuraten
- Updates vor Freigabe im gesamten Betrieb testen (z. B. in einer separaten Testumgebung) und die Testergebnisse mit dem BR besprechen

ONEDRIVE

OneDrive ist eine individuell gestaltbare Bibliothek zum Ablegen von Dateien aller Art. Im Speicher von OneDrive können sämtliche Dateiformate (z. B. Texte, Musik, Fotos, etc.) in selbst gestalteten Ordner-Systemen abgelegt werden. Da es sich um eine Anwendung in der Cloud handelt, können NutzerInnen von unterschiedlichen Orten jederzeit auf ihr persönliches Ordnersystem zugreifen und die Dokumente bearbeiten. Hat man weiteren Personen den Zugriff erlaubt, können die Dateien auch gemeinsam bearbeitet werden.

AdministratorInnen haben nicht automatisch Zugriff. Was prinzipiell von Vorteil ist, weil keine unberechtigte Einsicht oder Abänderung durch AdministratorInnen passieren kann, erweist sich in Notfällen, wenn Dateien dringend benötigt werden, als Nachteil. Dieses Zugriffsverbot für AdministratorInnen kann im Admin-Portal von MS 365 aber umgangen werden. Dazu wird für den/die BesitzerIn von OneDrive ein Link zum Admin festgelegt. NutzerInnen, die sich mit OneDrive sehr gut auskennen, können aber wiederum nachprüfen ob und wer sich bei ihrem OneDrive Zutritt verschafft hat. Dazu kommt man über den Klick „Websitesammlungsadministratoren" im Menüpunkt „Berechtigungen".

Außerdem tauchen sämtliche Zutritte auch im „Log-Protokoll" des Menüpunkt „Security & Compliance" auf. Wer also mit MS OneDrive sehr vertraut ist, kann seine Dokumente und allfällige unliebsame Einsichtnahmen überprüfen – wer weniger vertraut damit ist, wo welche Einstellungen und Informationen zu finden sind, der oder die muss darauf vertrauen, dass sich schon niemand einschleichen wird.

- Wie müssen die Passwörter aussehen?
- Zugriff regeln (Wer darf Einsicht nehmen/verändern? Wer darf im Abwesenheitsfall als Vertrauensperson Dokumente aus OneDrive nachsehen? Gibt es Gruppen-OneDrive? Ist alles für alle offen?)
- Wird regelmäßig überprüft, wer sich wessen OneDrive angesehen hat?
- Regeln für welche Dokumente OneDrive verwendet wird (z. B. keine Personalakten)
- Aufbewahrungsdauer festlegen („retention policy")

Haftung klären falls wichtige Dokumente „verschwinden" (ev. zusätzlich Data Loss Prevention [S. 46] in Betrieb nehmen)

- 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)
- Eventuell Freiwilligkeit vereinbaren

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

Eine Empfehlung für derartige externe Speicher kann nicht ausgesprochen werden, da sie sich fast immer in den USA befinden.

Ebenso wenig kann die Nutzung des Gratis-Angebots von OneDrive [S. 47] nahegelegt werden, da sich MS hier vorbehält, sämtliche Telemetriedaten mitzulesen.

AdministratorInnen können über die globalen MS Security and Compliance [S. 44] einrichten, dass personenbezogene Daten wie IP-Adressen, Betreff-Zeilen oder gar Inhalte *nicht* an MS übermittelt werden.

VISIO

Visio wurde von MS 2000 gekauft. Es ist Teil der MS 365 „Produktfamilie", also 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.

In einer BV zu regeln sind dabei insbesondere

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

SKYPE

Den „Kommunikations-und-Tratsch-Vorgänger" von Skype, den „Live Messenger" gibt es seit 2013 nicht mehr. Die Chat-Funktion wurde bei Skype eingebaut (bzw. wird über Yammer [S. 48] geplaudert, also „gechattet"). Doch auch für Skype ist seit 2017 klar, dass es nicht mehr lange leben wird. Mit 2021 geht Skype in Teams [S. 34] über.

Regeln zum Skypen sollten mit den Regeln für das Video-Telefonieren in Teams [S. 34] übereinstimmen.

Beim Chatten mittels kurzen Textnachrichten sollte generell Folgendes geklärt sein:

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

YAMMER

Über Yammer wird gechattet – man könnte es auch als „innerbetrieblichen Bassenatratsch" bezeichnen. In Yammer erstellen die Beschäftigten oder auch KundInnen und GeschäftsparnterInnen persönliche Profile. Die Gruppen können anhand ihrer jeweiligen Qualifikationen koordiniert werden. Relevante Personen, Inhalte und Unterhaltungen können über Graph [S. 38] gefunden werden. Nachdem die Verwendungszwecke, denen von MS Teams [S. 34] (bzw. außerhalb der MS-Welt denen von Facebook oder Xing) sehr ähnlich sind, gehen ExpertInnen davon aus, dass das Programm ein Ablaufdatum hat. Mittelfristig wird Yammer vermutlich in Teams aufgehen.

Yammer umfasst einige problematische Funktionen: Es kann explizit „Praise" – also Lob – über Yammer ausgetauscht werden; es können „einflussreiche" ArbeitnehmerInnen über Graph [S. 38] ermittelt werden; ein Präsenzstatus legt offen woran und wo Team-KollegInnen derzeit arbeiten.

Daher sollten bei der Verwendung von Yammer folgende Punkte klargestellt sein:

- „Lob" von Yammer deaktiveren
- Präsenzstatus ausschalten
- Auswertungs- und Benachteiligungsverbot
- Freiwillige Profile
- Zugriffe für einen eingeschränkten Personenkreis (nicht nach dem Prinzip „alle sehen alles")
- Zu kommunizierende Inhalte festlegen (z. B. keine besonders schützenswerten Daten, keine Krankmeldungen, keine Fahrtroutenänderungen, keine Schichtpläne, etc.)

CORTANA

Was „Alexa" für Amazon und „Siri" für Apple ist, das ist „Cortana" für Microsoft – ein so genannter „Sprachassistent", wobei die männliche Bezeichnung hier irreführend ist, handelt es sich doch bei den Assistenten in der Regel um weibliche Stimmen. Cortana ist eigentlich eine eigenständige Anwendung und kein Produkt innerhalb der MS 365-Palette. Der Sprachassistent wird hier nur der Vollständigkeit halber erwähnt, da MS 365-Anwendungen auch damit gesteuert werden können.

E-Mails per Sprachanweisung verschicken oder schreiben, Dokumente suchen, Termine abfragen, dazu ist Cortana da – hatte aber bislang, verglichen mit den anderen Freundinnen aus der Runde der Sprachassistentinnen eher bescheidene Kritiken. 2019 wurde Cortana für PrivatnutzerInnen überhaupt von Android- und Apple-Handys vom Markt genommen[55].

Ein Update von Mai 2020 soll Cortana wieder Auftrieb verschaffen, indem zusätzlich sprachgesteuert Termine im Kalender eingetragen werden können, an den Termin erinnert werden kann, Aufgaben aus der To-Do-App[56] abgerufen werden können sowie die Abfrage via der MS-eigenen Suchmaschine Bing möglich sein soll. Dieses Update ist in Europa derzeit nicht erhältlich (Stand November 2020). „Kunden von Microsoft 365 Enterprise mit englischsprachigen Exchange-Mailkonten bekommen automatisch eine Briefing-Funktion, bei der Cortana als intelligenter Assistent fungieren soll, der auf Termine und noch ausstehende Antworten hinweist" schreibt Heise online[57]. Der europäische Markt wird also offenbar Stück für Stück „Cortana-fit".

Bei einer BV zu Cortana 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

55 https://www.chip.de/news/Zeit-zu-gehen-Microsoft-nimmt-nervigen-Sprachassistenten-von-Android-und-Apple-Smartphones_177093989.html; 11.12.2020
56 ToDo ist eine MS365-App, die Aufgaben aus anderen Anwendungen übersichtlich zusammenfassen soll.
57 https://www.heise.de/news/Microsoft-bringt-neue-Funktionen-fuer-den-Sprachassistenten-Cortana-4767353.html ; 11.12.2020

CHECKLISTE: WIRD MS 365 IN EINKLANG MIT DER DSGVO GEBRACHT?

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

- ☐ Wurden die Betroffenen über die Datenverwendungen in MS 365 **informiert**? (Transparenzgebot, Informationspflicht)

- ☐ Wurde eine **Datenschutzfolgenabschätzung** vorgenommen?
  - ○ Wurde eine Risikobewertung für AN vorgenommen?
  - ○ Wurden die Betroffenen/der BR dabei befragt?
  - ○ Wurden Abhilfe geschaffen gegen allfällig bestehende Risiken?
  - ○ Ist der/die betriebliche Datenschutzbeauftragte eingebunden gewesen?

- ☐ Haben die Betroffenen **eingewilligt** – falls es sich um freiwillige Features handelt?
  - ○ Ist die Zustimmung zur Verwendung des MS-tools an die (Weiter-)Beschäftigung oder andere das Arbeitsverhältnis betreffende Faktoren gekoppelt?
  - ○ Sind die Nutzungsbedingungen in einer Betriebsvereinbarung so geregelt, dass den AN ein möglichst großer Spielraum zur freiwilligen und diskriminierungsfreien Verwendung einzelner Tools bleibt. (z. B. Ausschalten des Präsenzstatus, Ausschluss von Aufzeichnung, Archivierung, etc.)

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

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

- ☐ Wurde die **Rechenschaftspflicht** eingehalten, d.h. sind die Verwendungsvorgänge von MS 365 dokumentiert?

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

- ☐ **Überblick über im Betrieb verwendete Programme**/Tools/Anwendungen im Paket MS 365 (s: Technische Checkliste zum Einsatz von Microsoft 365) [S. 52]
- ☐ Klarstellung, dass einzelne Tools, die personenbezogene AN-Daten verarbeiten, in **Zusatz-Betriebsvereinbarungen** geregelt werden
- ☐ Umgang mit **Updates** (regelmäßige Testläufe in Bezug auf Auswirkungen auf die Privatsphäre der Beschäftigten)
- ☐ **Löschfristen** (so weit als möglich) bzw. organisatorische Maßnahmen, falls die Löschung technisch nicht möglich ist
- ☐ **Klares Berechtigungskonzept**
- ☐ Das Anzeigen von **Auswertungen** grundsätzlich einschränken (insbes. Delve [S. 37] und My Analytics [S. 39] ausschließen)
- ☐ **Kontrolle** von Einzelnen ausschließlich anlassbezogen (bei nachgewiesenem Fehlverhalten)
- ☐ **Heimliche/verdeckte Aktionen** unterbinden (z. B. auf Desktop Aufschalten, Mithören/Aufnehmen ...)
- ☐ Maßnahmen, die auf BV-widrigen Auswertungen und Kontrollen beruhen, sind **unwirksam** bzw. müssen zurückgenommen werden, ebenso verhält es sich mit allfälligen Benachteiligungen
- ☐ Erstellen von **Profilen** zur Leistungsbeurteilung (z. B. Ranking, Boni, etc.) unterbinden! Festlegen organisatorischer Maßnahmen, falls das Unterbinden des Erstellens von Profilen technisch nicht möglich ist
- ☐ **Transparenz** für ArbeitnehmerInnen: **Schulungen** anbieten, **Informationen** geben, AnsprechpartnerInnen im Unternehmen, Ansprechperson/Experteln für MS 365 im Betrieb ernennen
- ☐ Mitbestimmung des Betriebsrates im Prozess der **Einführung** und Adaptierung regeln (Empfehlung: Einrichtung einer Arbeitsgruppe MS 365 zur begleitenden Evaluierung)
- ☐ Regelmäßige **Evaluierung**
- ☐ **Freiwilligkeit** (so weit als möglich (z. B. OneDrive [S. 47]) aber zumindest bei Freigabe persönlicher Informationen (Profilfoto, Status, usw.)
- ☐ **Privatnutzung** regeln und zulassen (solange sie die betrieblichen Abläufe nicht stört und keine Schäden verursacht)
- ☐ **Datenschutzfolgenabschätzung**: Mitwirkung des Betriebsrates daran
- ☐ **Auftragsverarbeitervertrag** mit MS: Speicherort in Europa
    - ○ Einsicht in Auftragsverarbeitervertrag (bzw. OST)

TECHNISCHE CHECKLISTE ZUM EINSATZ VON MICROSOFT 365

1) In welcher Umgebung wird Microsoft 365 betrieben?

- on-premises
- hybrid
- Cloud

2) Welche MS 365 Variante ist im Einsatz?

- Microsoft 365 Enterprise E3/E5/F3
- Microsoft 365 Business Basic/Standard/Premium
- Microsoft 365 ProPlus (ausschließlich Apps)

3) Welche der folgenden **Komponenten/Services** zu MS 365 sind im Einsatz?

In dieser Tabelle sind die derzeit erhältlichen Anwendungen von MS 365 aufgelistet. Der Betriebsrat kann mit Hilfe der Tabelle nachfragen, ob die Anwendungen im Betrieb im Einsatz sind und hinterfragen, wozu, also für welchen Zweck das jeweilige Programm dient. (So sollte beispielsweise ein Kommunikationstool wie Teams der Kommunikation und nicht der Arbeitszeitkontrolle dienen.) Falls die Anwendung bisher nicht in der Broschüre erwähnt wurde, wird in der Fußnote kurz erklärt, wozu sie dient.

Außerdem ist die Liste nützlich um festzuhalten, ob für die jeweilige MS-Anwendung eine Betriebsvereinbarung – eventuell zusätzlich zu einer Rahmenvereinbarung – erforderlich ist.

Ein Beispiel: Die Komponente „Projekt 2019" soll im Sommer 2021 ausgerollt werden, weshalb die zweite Spalte mit einem Datum versehen wird. Der Verwendungszweck ist eine Personaleinsatzplanung, was in der dritten Spalte vermerkt wird. Da eine umfangreiche Datenverwendung und -auswertung der Beschäftigtendaten möglich ist (z. B. Qualifikationen, Multiprojektmanagement, Zeiterfassung, zentrale Ressourcenplanung, Risikomanagement, Dokumentenmanagement, Zugriffsverwaltung, Reporting, etc.), ist in der vierten Spalte ein „Ja" einzutragen. Und bei den Anmerkungen könnte man vorab getroffene Vereinbarungen oder kritische Punkte festhalten, wie z. B. „Zugriff nur für personalverantwortliche Führungskräfte nach umfassender Schulung".

Die ausgefüllte Tabelle ist ein gemeinsames Werkzeug von Betriebsrat und Geschäftsführung um den Überblick über die Anwendungen von MS 365 und die dazu erforderlichen Betriebsvereinbarungen zu behalten. Eine aktuelle Fassung davon stets zur Verfügung zu haben, ist sicherlich ein Vorteil.

Anwendung/Komponente	ja/nein/ geplant	Verwendungszweck/ Funktion	Betriebsver-einbarung ja/nein/in Arbeit	Anmerkungen
Office (Outlook, Word, Excel, PowerPoint, Access, Publisher)				
OneNote[1]				
Office Mobile				
Office Online				
Project 2019[2]				
Sway[3]				
Exchange Online				
Exchange Online Protection				
Data Loss Prevention				
eDiscovery				
SharePoint				
Yammer Enterprise				
Power App[4]				
Power Automate[5]				
Power BI[6]				
Retention Policy[7]				
OneDrive				
MyAnalytics[8]				
Flow				

1 OneNote ist eine App zum Organisieren von (handschriftlichen) Texten, Notizen, Bildern, etc. Übertragen von firmeneigenen Servern in die Cloud und umgekehrt wird über SharePoint [S. 42] und OneDrive [S. 47].
2 Project ist ein sehr umfangreiches Tool zur Planung, Steuerung und Überwachung von Projekten. MS Project 2019 enthält Qualifikationen, Multiprojekt-management, Zeiterfassung, zentrale Ressourcenplanung, Risikomanagement, Dokumentenmanagement, Zugriffsverwaltung, Reporting, etc., weshalb es jedenfalls einer Zusatz-BV bedarf.
3 Sway ist eine Software für Präsentationen. Die Daten werden in den USA gespeichert. Der Hessische DSB hat die Verwendung an Schulen untersagt.
4 Mittels Power App können Arbeitsabläufe vordefiniert und angestoßen werden (z. B. Urlaubsantrag, Abwesenheitsnotiz).
5 Über Power Automate können selbst definierte Abläufe zwischen verschiedenen Anwendungen programmiert werden (z. B. automatische Regeln für das Organisieren von Dokumenten aus Outlook in OneDrive, automatische Push-Mails wenn bestimmte Personen etwas twittern, Benachrichtigung sobald etwas in die DropBox gestellt wird, u.s.w.).
6 PowerBI ist ein Programm zur grafischen Darstellung von statistischen Daten (z. B. Excel-Tabellen, Datenbanken). Mit Power BI können Reports über das Nutzungsverhalten der Beschäftigten in – beinahe – beliebigem Umfang dargestellt werden (z. B. in welchem Ausmaß wurde OneDrive genutzt?).
7 Die „retention policies" bestimmen, für welche Dauer Dinge im „permanenten Archiv" gelagert bleiben.
8 Eigentlich ist es nicht ratsam, Analytics zu aktivieren. Sollte es dennoch unbedingt gewünscht sein, sollte es nur freiwillig erfolgen und ausschließlich der ganz persönlichen Analyse des Arbeitsverhaltens dienen. Die Empfehlungen von MS sind keinesfalls als Arbeitsvorgaben, Leistungsbewertungen oder Ähnliches zu interpretieren.

Anwendung/Komponente	ja/nein/ geplant	Verwendungszweck/ Funktion	Betriebsver-einbarung ja/nein/in Arbeit	Anmerkungen
Stream				
Skype				
Meeting Broadcast				
Forms[9]				
Audit Logging				
Teams				
Planner[10]				
Delve[11]				
ToDo[12]				
Kaizala[13]				
Audio Conferencing				
Phone System				
Identity and Threat Protection				
Information Protection & Compliance				
Visio				
Enterprise Mobility and Security (EMS)[14]				
Azure Active Directory				
Intune				
System Center Configuration Manager				
Microsoft Cloud App Security				

9 Forms ist eine Software zur Erstellung von Umfragen oder Formularen.
10 Planner ist eine Software zum Planen von Teamarbeit. Planner gibt es nicht als Desktop-Anwendung, sondern nur als mobile App.
11 Eigentlich ist es nicht anzuraten, Delve zu aktivieren. Sollte es dennoch unbedingt gewünscht sein, wäre die Suche nach relevanten Dokumenten die einzig einigermaßen sinnvolle Anwendung.
12 To-Do hieß vor dem Kauf durch MS „Wunderlist" und ist eine App um Aufgaben aus anderen Programmen (Outlook, Planner) zu einem eigenen, nur individuell einsehbaren Tagesplan zusammenzustellen.
13 Kaizala ist ein einfaches Chatprogramm für Smartphones. Wurde vor allem für Schwellenländer als Alternative zu WhatsApp entwickelt und soll ab 2020 nicht mehr serviciert werden.
14 In der EMS wird die Sicherheit für mobile Geräte und Anwendungen verwaltet. Der Zugriff darauf sollte unbedingt auf die IT-Abteilungen beschränkt sein und personenbezogene Auswertungen sollten ausschließlich bei begründetem Verdacht im Anlassfall zugelassen sein.

Anwendung/Komponente	ja/nein/ geplant	Verwendungszweck/ Funktion	Betriebsver-einbarung ja/nein/in Arbeit	Anmerkungen
Azure Information Protection				
Multi-Factor Authentication				
Advanced Threat Analytics				
Azure Advanced Threat Protection				
Identitäts-Manager				

Security and Compliance Center (SCC)[15]

Access to the Security & Compliance Center				
Office 365 Cloud App Security				
Threat management[16]				
Advanced threat management[17]				
Customer Lockbox				
Mobile device management				
Data loss prevention for Exchange, SharePoint, OneDrive for Business, Teams chat and channel messages				
Information barriers				
Data governance				
Advanced data governance				
Content search				
eDiscovery				
Advanced eDiscovery				
Archiv				
Unified auditing				
Supervision policies				

15 Im Security & Compliance Center können sämtliche Aktivitäten überwacht werden. Der Zugriff darauf ist jedenfalls auf die IT-Abteilungen zu beschränken und personenbezogene Auswertungen nur im Anlassfall zuzulassen.
16 Threat Management dient dem Filtern von Emails um Gefahren abzuwenden.
17 Mit Threat Management Advanced können eigene Kampagnen erstellt werden (z. B. gegen Phishing generell) um Gefahren abzuwehren.

WEITERFÜHRENDE UNTERLAGEN DER GEWERKSCHAFT GPA UND ANDERER INTERESSENVERTRETUNGEN

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. 34])
- Muster-BV Dokumentenmanagement (OneDrive [S. 47], Delve [S. 37])
- Muster-BV Mobile Device Management (Enterprise Mobility Suite, EMS, Outlook Mobile [S. 32])
- Muster-BV Zutritt (Security & Compliance [S. 44], One Drive [S. 47])
- Leitfaden Mitarbeiterumfrage (Forms)
- Muster-Module Videokonferenzsystem (Teams [S. 34])
- Checkliste Rankings (My Analytics/Workplace Analytics [S. 39])
- Arbeitsunterlage Einsicht in E-Mails (z. B. für Outlook [S. 32], Teams [S. 34])
- Muster Rahmen-BV

u.s.w.

Hans Böckler Stiftung (2018) Nils Werner: Einführung und Anwendung von Office 365;
https://www.boeckler.de/pdf/mbf_bvd_praxis_office_365.pdf

Hans Böckler Stiftung (2018) Manuela Maschke (Hg.) Heinz-Peter Höller,
Peter Wedde: Vermessung der Belegschaft, Mining the Enterprise Social Graph

JETZT MITGLIED WERDEN!

Familienname..... Vorname..... ☐ Frau ☐ Herr

Geburtsdatum | | | | | | | | | Titel ..... Geburtsname .....

Straße/Haus-Nr. ..... PLZ/Wohnort.....

Telefonisch erreichbar ..... E-Mail.....

☐ Angestellte/r ☐ Lehrling ☐ Werkvertrag ☐ geringfügig beschäftigt ☐ Freier Dienstvertrag ☐ Selbstständig (Gewerbeschein)
☐ Zeitarbeitskraft ☐ SchülerIn ☐ StudentIn ☐ dzt. ohne Beschäftigung ☐ Zweitmitgliedschaft ☐ FacharbeiterIn

Derzeitige Tätigkeit ..... ☐ Ich war bereits Mitglied der Gewerkschaft von/bis .....

Beschäftigt bei Firma (bzw. Schule/Universität)..... Dienstort .....

Anschrift.....

Branche .....

Höhe des monatlichen Beitrages: **EUR** | | | | | | **BEITRITTSMONAT/-JAHR** | | | | | | |

Der monatliche Mitgliedsbeitrag beträgt 1% des Bruttogehalts bis zu einem Maximalbeitrag (siehe **www.gpa.at/mitgliedsbeitrag**), der jährlich angepasst wird. 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 Mitgliedsbeitrags erfolgt jeweils zum Monatsultimo.

☐ monatlich ☐ alle 2 Monate ☐ jedes Quartal ☐ 1/2 jährlich ☐ jährlich (Schüler-/StudentInnen, Zweitmitgliedschaft)

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, umseits stehende Datenschutzerklärung (auch abrufbar unter **www.oegb.at/datenschutz**) zur Kenntnis genommen zu haben.

.....
Datum/Unterschrift

1030 Wien, Alfred-Dallinger-Platz 1, Service-Hotline: +43 (0)5 0301,
E-Mail: service@gpa.at, ZVR 576439352, CID: AT48ZZZ00000006541

WerberIn-Mitgliedsnummer:.....

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 Österreichische Gewerkschaftsbund (ÖGB)/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 umseits 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/Gewerkschaft GPA; soweit Sie dem Betriebsabzug zugestimmt haben, Ihre Einwilligung zur Verarbeitung der dafür zusätzlich erforderlichen Daten.

Die Datenverarbeitung erfolgt durch den ÖGB/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/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

MITMACHEN – MITREDEN – MITBESTIMMEN

INTERESSENGEMEINSCHAFTEN DER GEWERKSCHAFT GPA bringen Menschen mit ähnlichen Berufsmerkmalen zusammen. Zum Austauschen von Erfahrungen und Wissen, zum Diskutieren von Problemen, zum Suchen kompetenter Lösungen, zum Durchsetzen gemeinsamer beruflicher Interessen.

Mit Ihrer persönlichen Eintragung in eine oder mehrere berufliche Interessengemeinschaften

- erhalten Sie mittels Newsletter (elektronisch oder brieflich) regelmäßig Informationen über Anliegen, Aktivitäten und Einladungen für Ihre Berufsgruppe;
- können Sie Ihre beruflichen Interessen auf direktem Weg in die Kollektivvertragsverhandlungen Ihres Branchenbereichs einbringen;
- erschließen Sie sich Mitwirkungsmöglichkeiten an Projekten, Bildungsveranstaltungen, Kampagnen, Internet-Foren und anderen für Ihre Berufsgruppe maßgeschneiderten Veranstaltungen, auch auf regionaler Ebene;
- nehmen Sie von der Interessengemeinschaft entwickelte berufsspezifische Dienstleistungen und Produkte in Anspruch (Fachberatung auf regionaler Ebene, Bücher, Broschüren und andere Materialien);
- beteiligen Sie sich an demokratischen Direktwahlen Ihrer beruflichen Vertretung auf Bundesebene sowie regionaler Ebene und nehmen dadurch Einfluss auf die gewerkschaftliche Meinungsbildung und Entscheidung.

Nähere Infos dazu unter: **www.gpa.at/interesse**

ICH MÖCHTE MICH IN FOLGENDE INTERESSENGEMEINSCHAFTEN EINTRAGEN:

☐ **IG PROFESSIONAL** ☐ **IG FLEX** ☐ **IG SOCIAL** ☐ **IG IT** ☐ **IG EXTERNAL** ☐ **IG POINT-OF-SALE** ☐ **IG MIGRATION** ☐ **IG EDUCATION**

Dieses Service ist für mich kostenlos und kann jederzeit von mir widerrufen werden.

☐ Frau ☐ Herr Titel .....

Familienname..... Vorname.....

Straße/Haus-Nr. ..... PLZ/Wohnort.....

Berufsbezeichnung..... Betrieb .....

Telefonisch erreichbar ..... E-Mail.....

.....
Datum/Unterschrift

MEINE GEWERKSCHAFT

GEWERKSCHAFT GPA
IN GANZ ÖSTERREICH

SERVICE-HOTLINE:
+43 (0)5 0301

GEWERKSCHAFT GPA
Service-Center
1030 Wien, Alfred-Dallinger-Platz 1
Fax: +43 (0)5 0301
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!