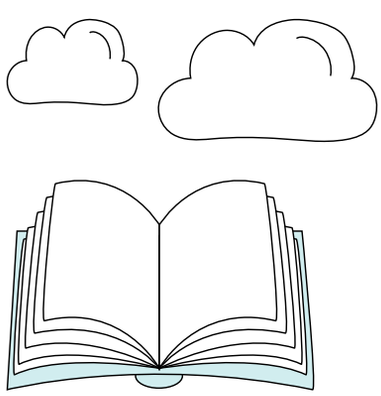
MORGENSTERN

Whitepaper

Rechtssicherer Umgang mit Microsoft 365



morgenstern-legal.com

morgenstern-privacy.com

Inhalt

Wir bei MORGENSTERN legen großen Wert auf inklusive Sprache. Deswegen gendern wir – und zwar gerne! Du sollst dich von unseren Texten angesprochen fühlen, egal wer du bist.

Fachbegriffe gendern wir jedoch nicht, da sie wie Eigennamen feststehende Begriffe sind. Hier geht es nicht um das generische Maskulinum, sondern um fachliches Vokabular, das seine eigene juristische Bedeutung hat.

...dir aber nun **viel Spaß**, liebe*r Leser*in!

01. Einführung

Microsoft 365, eine auf den ersten Blick harmlose „Bürosoftware“, muss seit geraumer Zeit viel Kritik einstecken, und zwar von Seiten der Datenschützer*innen sowie von der Front der Arbeitsrechtler*innen.

Dieses Whitepaper stellt für dich die wichtigsten Vorgaben, Handlungsempfehlungen und Hintergründe zusammen. Bitte bedenke dabei aber immer, dass dies nur ein Leitfaden sein kann, der ausdrücklich nicht den Anspruch erhebt, eine rechtliche Beratung darzustellen oder zu ersetzen.

Falls du tiefergehende Fragen hast, komm gerne auf uns zu!

Brauchst du Rat? Kontaktiere uns! Wir bei MORGENSTERN haben ein erfahrenes und hoch spezialisiertes Team bestehend aus Anwälten und Anwältinnen sowie Datenschutz- und IT-Sicherheitsexpertinnen und -experten!

contact@morgenstern-privacy.com
+49 (0) 6232 - 100119 44

Microsoft 365 -
MORGENSTERN Packages

Mehr MORGENSTERN Whitepaper findest du übrigens auch unter:
morgenstern-privacy.com & morgenstern-legal.com

Was macht die Einführung der Produkte so herausfordernd?

In den Funktionsumfang der Microsoft 365-Produktsuite sind Verfahren eingebunden, die sowohl aus rechtlicher, als auch aus (IT-)Compliance-technischer Sicht einer gewissenhaften und sorgfältigen Vorprüfung und Risikoanalyse bedürfen.

Nach den neuesten Feststellungen der Datenschutzkonferenz (DSK) (Stand: 24. November 2022) sei zudem ein durchgehend rechtssicherer bzw. datenschutzkonformer Betrieb und Einsatz von Microsoft 365 auf Basis des Standard-Auftragsverarbeitungsvertrags von Microsoft nicht möglich. Dieser Meinung sind die Behörden auch nach zahlreichen Änderungen, die Microsoft nach vielen Gesprächen mit der Datenschutzkonferenz in seinen Vertragswerken umgesetzt hat.
Grundlage der Ergebnisse dieser Bewertung der DSK ist dabei allerdings nur der „Datenschutznachtrag zu den Produkten und Services von Microsoft" (sog. „Datenschutznachtrag") in der Fassung vom 15. September 2022, der unter anderem den Auftragsverarbeitungsvertrag enthält. Die Datenschutzkonferenz kam konkret zu dem Ergebnis, dass Verantwortliche den Nachweis, Microsoft 365 datenschutzkonform zu betreiben, auf Grundlage dieses Datenschutznachtrags nicht führen können.

Der Bericht der Datenschutzkonferenz soll ausdrücklich keine abschließende Untersuchung und insbesondere keine vollständige datenschutzrechtliche Bewertung des Cloud-Dienstes Microsoft 365 darstellen. Eine solche Prüfung bleibt daher Aufgabe der Behörden bzw. der Unternehmen, die Microsoft 365 einsetzen wollen. Prüfungsmaßstab für die Festlegungen der DSK ist allein die Frage, ob der Datenschutznachtrag die Anforderungen des Art. 28 Abs. 3 DS-GVO sowie die vom Europäischen Gerichtshof im Schrems II Urteil aufgestellten Maßstäbe zum Drittstaatentransfer erfüllt. Jedenfalls letztere Frage hat sich seit dem 10.07.2023 mit dem Erlass des Angemessenheitsbeschluss (EU-U.S. Data Privacy Framework) durch die Europäische Kommission – zumindest vorerst – „erledigt". Microsoft hat seine Zertifizierung nach dem EU-U.S. Data Privacy Framework bereits kurze Zeit nach dem Inkrafttreten des Abkommens aktualisiert und mittlerweile auch bereits im neuen Datenschutznachtrag implementiert (Stand: 15.November 2023).

Hintergrundwissen: Drittstaatentransfer
Möchte eine verantwortliche Stelle personenbezogene Daten in ein sogenanntes Drittland – also einen Staat außerhalb der EU/des EWR – übermitteln, muss diese zunächst die gesetzlichen Hürden der Art. 44 ff. DS-GVO überwinden. Der Gesetzgeber möchte damit sicherstellen, dass das von der DS-GVO vorgeschriebene Schutzniveau auch dann auch dann gewahrt bleibt, wenn die Daten in ein Land gelangen, in dem andere Gesetze mit einem möglicherweise geringeren Datenschutzniveau Anwendung finden. Für einige Staaten (oder bestimmte Sektoren oder Gebiete) hat die Europäische Kommission bereits geprüft und auf dieser Grundlage entschieden, dass personenbezogene Daten in dem jeweiligen Staat ein angemessenes Schutzniveau genießen, das mit dem der Datenschutz-Grundverordnung vergleichbar ist. Diese Entscheidung wird als Angemessenheitsbeschluss bezeichnet.

Sollen Daten in ein Drittland übermittelt werden, für das kein solcher Angemessenheitsbeschluss vorliegt, liegt es weitestgehend in der Verantwortung der transferierenden Unternehmen und Behören, durch sogenannte geeignete Garantien ein angemessenes Datenschutzniveau bei der Verarbeitung im Drittland sicherzustellen.

Zu den gängigsten Garantien gehört der Abschluss der Standarddatenschutzklauseln der EU-Kommission. Dabei handelt es sich um vertragliche Vereinbarungen, die mit einem Unternehmen in einem Drittland geschlossen werden können und die dazu führen, dass sich das Unternehmen in dem Drittland zur Einhaltung eines angemessenen Datenschutzniveaus verpflichtet.

Das Problem bei Verträgen ist jedoch, dass sie nur zwischen den Vertragsparteien gelten und Gesetze nur bedingt aushebeln können. Deshalb sehen die Standarddatenschutzklauseln zusätzlich vor, dass die übermittelnde Stelle prüft, ob im Drittland ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet ist. Das heißt konkret, man muss sich mit der Rechtslage und der Behördenpraxis des Landes auseinandersetzen und dies in einem sogenannten Transfer Impact Assessment dokumentieren. Kommt man zu dem Ergebnis, dass es um den Datenschutz nicht so gut bestellt ist (wie z.B. in den USA), muss man zusätzliche Maßnahmen ergreifen, um dies „auszugleichen", also den Zugriff durch Behörden und andere Stellen zu minimieren.

Und damit zurück zu Microsoft: Bisher musste man, seit der Europäische Gerichtshof im Juli 2020 das Privacy Shield gekippt hat, diesen ganzen oben beschriebenen Aufwand betreiben, wenn man Daten mit den Cloud-Diensten von Microsoft 365 sicher in die USA übertragen wollte. Seit dem 10.07.2023 hat sich die Situation diesbezüglich entspannt. Personenbezogene Daten dürfen nun an Microsoft als zertifiziertes Unternehmen übermittelt werden.

Doch leider ist es gut möglich, dass diese Rechtslage nicht lange Bestand haben wird: Die NOYB, eine Nichtregierungsorganisation, hat bereits angekündigt, dass das EU-U.S. Data Privacy Framework gerichtlich überprüft werden soll. Hiermit hatte die NOYB unter Max Schrems bereits zwei Mal Erfolg bei den Vorgängern des EU-U.S. Data Privacy Frameworks, weswegen die darauf basierenden Urteile auch als „Schrems I" und „Schrems II" bezeichnet werden.

Obwohl der Geltungsbereich dieser Feststellungen damit stark begrenzt ist und die Bewertung teilweise mehr oder weniger undifferenziert erfolgte, ist festzuhalten, dass der Einsatz mancher Einzelprodukte aus dem Microsoft 365-Portfolio tatsächlich erheblichen datenschutzrechtlichen sowie arbeits- und geheimhaltungsrechtlichen Bedenken begegnet.

Bei jeglicher, teilweise wohl auch berechtigter, Kritik an Microsoft 365 ist aber festzustellen, dass durch sachgerechte auch rechtliche) Evaluation des individuell gewünschten Funktionsumfangs von Microsoft 365 und die darauf aufbauende, passgenaue Ergreifung technischer und organisatorischer Maßnahmen (insbesondere der Anwendung des Grundsatzes Privacy by Design und Privacy by Default) wohl ein weitgehend rechtskonformer Einsatz von Microsoft 365 möglich sein wird.

Nachfolgend soll dargestellt werden, wo die konkreten Gefahren von Microsoft 365 liegen und wie ein solcher Einsatz gelingen kann.

02. Allgemeines zu Microsoft 365

Überblick

Um feststellen zu können, welche konkreten Maßnahmen zu ergreifen sind – insbesondere um entscheiden zu können, ob die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich ist – muss genau beschrieben werden, in welcher Edition, Version und mit welchen Konfigurationen sowie unter welcher Einsatzumgebung (z.B. ggfs. zusätzliche Verwendung von Windows 10) Microsoft 365 eingesetzt werden soll. Mit diesen Informationen können dann auch erst der Funktionsumfang und die Datenübermittlung an Microsoft bestimmt werden.

Sämtliche genutzte Funktionen und die eingesetzte Version sollten in einer Anlage dokumentiert werden. Diese kann dann als Grundlage für sämtliche rechtliche und sicherheitstechnische Prüfungen herangezogen werden.

icrosoft 365 bietet das Office-Paket für Windows, MacOS, iOS, Android sowie Windows Phone an. Das Paket bündelt verschiedene Anwendungsprogramme (z.B. Word, Excel, Outlook, etc.) von Microsoft. Microsoft 365 kann im Allgemeinen dabei auf folgende Weise genutzt werden:

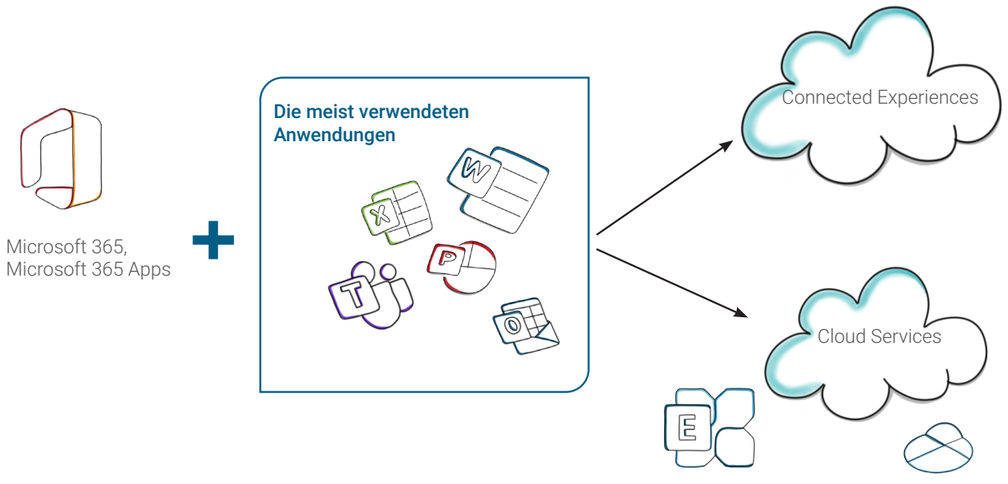
- lokal installiert auf den Computern und Laptops der Benutzer mit cloudbasierten Anwendungen
- installiert auf Smartphones und Tablets (mobile Office-Apps für iOS und Android)
- in Form von Online-Apps, die im Browser ausgeführt werden (Office Online)

Bei allen drei Arten der Nutzung besteht außerdem Zugriff auf Online-Mikroservices (z.B. Rechtschreibprüfung, Übersetzungstool, Möglichkeit, Bilder aus dem Internet einzufügen), die als Connected Experiences (verbundene Dienste) bezeichnet werden.

Microsoft selbst beschreibt die Produktsuite auf der Webseite so:

> „Microsoft 365 ist die leistungsfähige Produktivitätsplattform in der Cloud, die Anwendungen wie Microsoft Teams, Word, Excel, PowerPoint, Outlook, OneDrive sowie intelligente Clouddienste und erweiterte Sicherheit umfasst."
>
> https://www.microsoft.com/de-de/microsoft-365/microsoft-office
> zuletzt aufgerufen am 24.11.2023, 14:48 Uhr

Die Privacy Company hat für die niederländische Regierung im Zuge der beabsichtigten Einführung von Microsoft 365 bei den Behörden eine Datenschutz-Folgenabschätzung durchgeführt (dazu unten mehr). Die unterschiedlichen Anwendungen wurden von der Privacy Company wie folgt grafisch unterteilt (Risiken bei der Verarbeitung von Diagnosedaten):



Die Funktionen der fünf meist verwendeten Programme Word, Excel, PowerPoint, Outlook und Teams sind der Mehrheit der Nutzer*innen wohl gut bekannt.

Auf die Funktionen und (datenschutz-)rechtlichen Risiken bei der Nutzung der Microsoft-Cloud generell, samt den verbundenen Cloud-Services, der Nutzung von Microsoft Teams, weiterer ausgewählter Anwendungen sowie den sog. Connected Experiences, soll dagegen nachfolgend näher eingegangen werden.

03. Einzelne Anwendungen

SharePoint

SharePoint ist eine Plattform für die ortsunabhängige Online-Zusammenarbeit zwischen mehreren Nutzerinnen und Nutzern an gemeinsamen Projekten.

Die Anwendung wird als Webservice bereitgestellt, sodass von überall auf Arbeitsressourcen zugegriffen werden kann. SharePoint hat außerdem Social-Media-Funktionen, wie z. B. Blogs oder Diskussionsportale. Mit SharePoint können Informationen geteilt, kann kommuniziert, können Kalender gemeinsam oder alleine genutzt oder können Recherchen durchgeführt werden (etc.).

Fraglich ist in diesem Zusammenhang, inwieweit die Nutzung von SharePoint gegenüber dem Einsatz von Teams als gemeinsamem Workspace abgegrenzt werden kann. Die Einsatzmöglichkeiten überschneiden sich hier naturgemäß.

OneDrive

OneDrive ist ein Filehosting-Dienst bzw. ein persönlicher Cloud-Speicher, der es erlaubt, Daten nicht auf einem lokalen Datenträger, sondern auf den Servern von Microsoft zu speichern. Diese Daten können dadurch ortsunabhängig abgerufen werden (z. B. via Webbrowser oder Client).

Teams

Teams ist eine cloudbasierte Plattform, die Chat, Besprechungen, Notizfunktionen und Anhangmöglichkeiten kombiniert und damit die kollaborative Zusammenarbeit ermöglicht. Als Grundlage dienen Arbeitsbereiche, die aus verschiedenen Komponenten bestehen:

Workspace

Ein Workspace ist ein abgegrenzter Arbeitsbereich für ein festgelegtes Team, in dem alle Funktionen in Teams gemeinsam genutzt werden können. Es ist insbesondere möglich, Dateien gemeinsam zu erstellen und zur gemeinsamen Bearbeitung in Teams (einschließlich der Möglichkeit der Freigabe in SharePoint) abzulegen. Die Teams-Workspaces dienen damit zugleich der Bestimmung und Abgrenzung von Zugriffsberechtigungen.

Channels und Tabs

Eine weitere Komponente stellen die sog. Channels (Kanäle) dar, die als kleinere Untereinheit eines Workspace verstanden werden können. Es gibt öffentliche Kanäle und private Kanäle. Die Kanäle können wiederum in „Tabs“ unterteilt werden.

Teams basiert damit auf einer Art Team-Messenger bzw. auf Arbeitsbereichen.

Teams lässt sich vor allem in die anderen Microsoft 365-Anwendungen integrieren. Es hat insbesondere einen integrierten Zugriff auf teamspezifische Kalender, Dateien, OneNote-Notizen, Planner-Pläne, Schichtpläne, etc. Über Teams können auch Exchange Online und SharePoint Online genutzt werden, um eine gemeinsame Bearbeitung von Dokumenten und anderen Inhalten zu ermöglichen.

Hervorzuheben ist bei Teams zudem die Funktion „Videotelefonie“ bzw. „Videokonferenzen“. Mit diesen Funktionen können zwei oder mehr Nutzer*innen mittels Bildübertragung miteinander kommunizieren. Hier ist standardmäßig die Möglichkeit gegeben, die jeweiligen Sitzungen aufzuzeichnen, sodass Videos der Teilnehmer*innen gespeichert und zu einem späteren Zeitpunkt abgerufen werden können. Die Mitarbeitenden können diese dann jederzeit abrufen und abspielen, wobei der Kreis der Zuhörer*innen beschränkt werden kann. Der Streamingdienst ermöglicht es auch, die Inhalte in eine andere Sprache übersetzen zu lassen.
Darüber hinaus kann auf Teams auch über den Webbrowser zugegriffen werden. Bei dieser Zugriffsmethode besteht das erhöhte Risiko, dass Mitarbeitende im Rahmen von Phishing-Kampagnen auf gefälschte Login-Seiten geführt werden und dort ihre Login-Daten preisgeben.

Aus der Verwendung von Teams ergeben sich darüber hinaus folgende Risiken:

- Eine unzulässige Verhaltens- und Leistungskontrolle durch den Arbeitgeber und der dadurch entstehende Überwachungsdruck für die Beschäftigten wird z. B. durch die Anzeige des „Free/Busy“-Erreichbarkeits-Status der Nutzer*innen verschärft.

- Durch die Audio- und / oder Video-Aufnahme eines Meetings können Beschäftigte sich „beobachtet“ fühlen, was eine Verhaltenssteuerung der Mitarbeitenden zur Folge haben kann. Das Risiko, dass fremde unbefugte Personen, die Zugang zu Einladungslinks erhalten, sich auf eine Konferenz aufschalten oder Zugang zu personenbezogenen Daten in einem Workspace erlangen können, besteht insbesondere bei der Nutzung von Teams.

OneNote

Bei OneNote handelt es sich um eine Anwendung zur Erstellung und Organisation von digitalen Notizen.

Die betriebliche Nutzung von OneNote birgt insbesondere das Risiko, dass Daten, die von einer Cloud-Datenhaltung ausgeschlossen wurden, gleichwohl in der Microsoft-Cloud landen, weil die lokale Speicherung von Notizen mit OneNote nicht vorgesehen ist. Damit bestehen alle vorbeschriebenen Risiken, die sich aus der Cloud-Nutzung selbst ergeben, sodass der Ausschluss von Hoch-Risikodaten aus der Cloud umgangen werden würde.

Viva

Microsoft Viva ist eine Employee Experience Platform (EXP), die Kommunikation, Fachwissen, Lernen, Ressourcen und Erkenntnisse in den täglichen Arbeitsablauf einbinden soll.
Viva besteht aus den fünf Modulen

- “Viva Learning“,
- “Viva Insights”,
- “Viva Topics“,
- “Viva Connections“ und
- “Viva Goals”

Viva Learning

Viva Learning ist ein Modul von Viva, aus dem Mitarbeitende Lerninhalte aus den Bibliotheken des Unternehmens oder von externen Anbietern beziehen und nachverfolgen können.

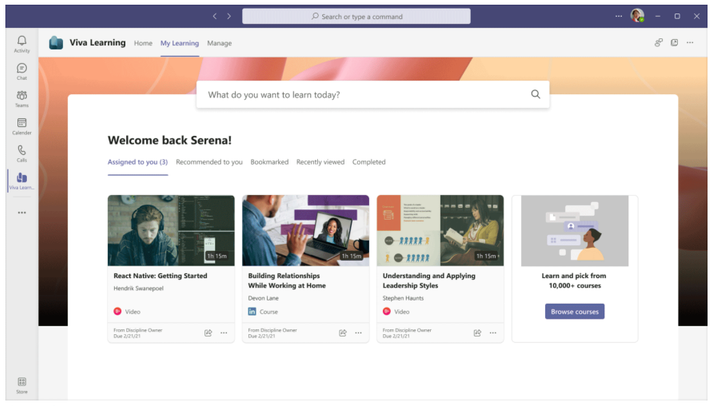


Abb. 1

Über Viva Learning können zum Beispiel Kurse von Microsoft Learn, LinkedIn oder Udacity gebucht werden. Viva Learning ist in Teams eingebunden, sodass eine Interaktion oder gemeinsames Lernen mit anderen möglich ist.

Viva Insights

Viva Insights bietet persönliche Einblicke sowie Einblicke durch Vorgesetzte in die Arbeitsgewohnheiten.

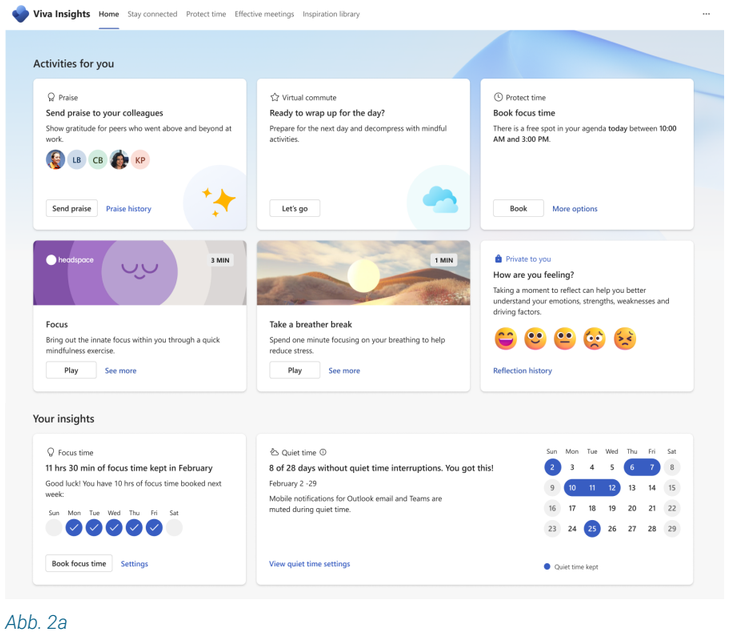


Abb. 2a

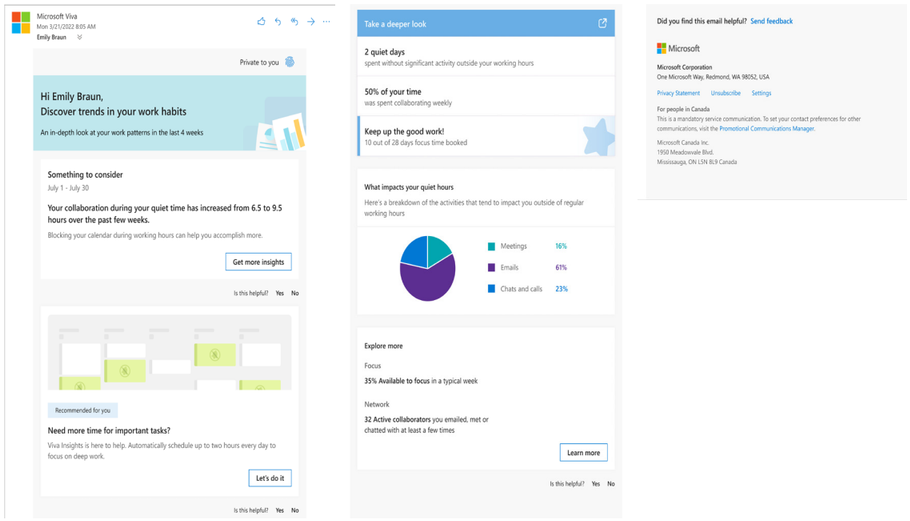


Abb. 2b

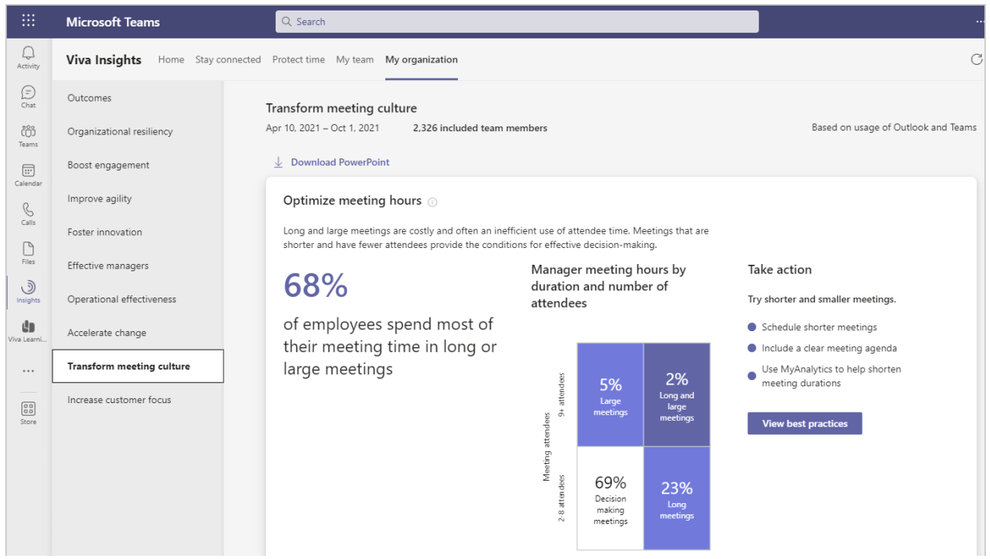


Abb. 3

Viva Insights analysiert die Arbeitsweise der Mitarbeitenden und gibt den Vorgesetzten damit sehr detaillierte Einblicke in ihre Tätigkeiten, was datenschutzrechtlich als äußerst kritisch zu bewerten ist und nicht pauschal empfohlen werden kann. So können etwa einzelne Mitarbeitende oder Gruppen von Mitarbeitenden mit anderen im Unternehmen verglichen werden („Peervergleich"):

Die Abfragen zu den Mitarbeitenden lassen sich zusätzlich anhand von bestimmten Filtern und Auswahlkriterien, wie z.B. deren Einsatzbereich, eingrenzen oder erweitern:

> *„Die Peervergleichsabfrage in Microsoft Viva Insights kann Ihnen dabei helfen, das Verhalten der Zusammenarbeit am Arbeitsplatz in Ihrer Organisation zu analysieren. Sie verwenden diese Art von Abfrage, um das Zusammenarbeitsverhalten einer oder mehrerer Peergruppen mit einer ausgewählten Anzahl von Personen zu vergleichen.*
>
> *Sie verwenden eine Peervergleichsabfrage, um Personen zu identifizieren, die auf bestimmte Weise mit anderen Personen vergleichen. Beim Erstellen der Abfrage identifizieren Sie die interessierten Personen, die Gruppen, mit denen sie verglichen werden sollen, die Vergleichsmetriken und einen Zeitraum, für den Daten abgerufen werden sollen. Beachten Sie, dass Personen während der Abfrage in der Ausgabe nicht identifiziert werden. Ergebnisse zeigen nur PersonIds an.*
>
> *Peervergleichsabfragen konzentrieren sich zwar auf Personen, erzeugen aber andere Informationen als Personenabfragen. Verwenden Sie eine Personenabfrage, um die Beziehung zwischen den Organisationsattributen einer Person, z. B. ihrem Team, ihrer Ebene oder ihrem Standort, zu verstehen und zu verstehen, wie sie ihre Zeit verwendet, oder wenn Sie wissen möchten, wie sich ein Aspekt ihrer Zeitzuweisung am Arbeitsplatz auf andere Aspekte ihrer Zeitzuweisung auswirken kann. Verwenden Sie eine Peervergleichsabfrage, um das Zusammenarbeitsverhalten der Person mit diesem Verhalten in den Peergruppen der Person zu vergleichen."*

Die Abfragen zu den Mitarbeitenden lassen sich zusätzlich anhand von bestimmten Filtern und Auswahlkriterien, wie z.B. deren Einsatzbereich, eingrenzen oder erweitern:

Der Zweck einer Peervergleichsabfrage besteht darin, Aspekte des Arbeitsverhaltens bestimmter Mitarbeiter in den Fokus zu rücken, indem sie mit anderen Personen in der Organisation, anderen in einer ihrer Peergruppen verglichen werden. Im Schritt „Mitarbeiter auswählen" wählen Sie diese Personen aus. (Sie wählen auch die anderen Personen aus, z. B. die Personen, mit denen Sie sie im Schritt „Peergruppen auswählen" vergleichen.)

Um die Personen auszuwählen, die Sie abfragen, filtern Sie sie nach ihren HR-Attributen, z. B.:

- *Domäne: Auswählen aller Personen, deren E-Mail-Adressen über eine bestimmte Domäne verfügen*
- *HourlyRate: Auswählen aller Mitarbeiter, die einen bestimmten Betrag verdienen*
- *FunctionType: Wählen Sie z. B. alle Ingenieure oder alle Personaler aus.*
- *Organisation: Auswählen aller Personen in einer oder mehreren Organisationen, z. B. Einrichtungen und Finanzen*

Mitarbeitende erhalten aber auch Einblicke in ihre eigenen Arbeitsgewohnheiten. Sie bekommen beispielsweise Vorschläge zu Pausen, der Reduzierung von Unterbrechungen („Fokuszeit") oder eine Übersicht dazu, wie viel Zeit sie mit bestimmen Anwendungen oder Personen verbringen. Viva Insights analysiert zudem KI-basiert die E-Mail-Kommunikation nach bestimmten Schlüsselwörtern oder Aussagen.

So zeigt Insights etwa einzelne Auszüge aus E-Mails an, die auf Vereinbarungen, Zusagen, Fragen oder Termindaten hinweisen:

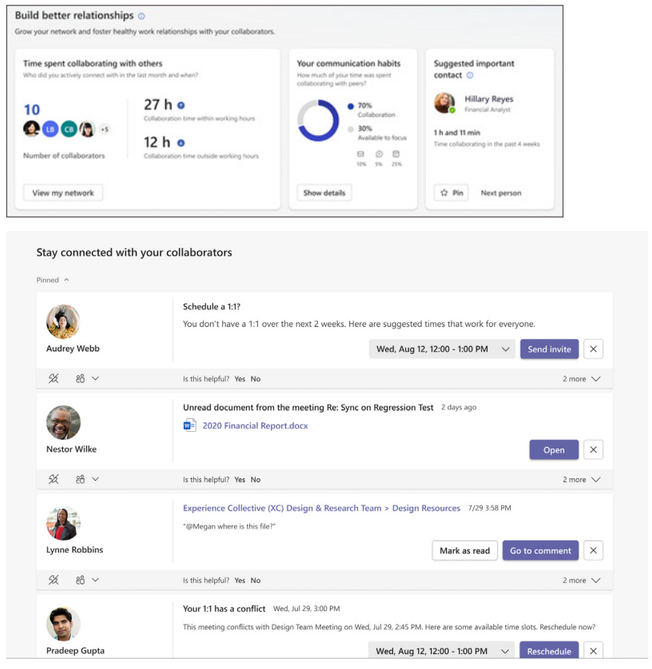


Abb. 4

Viva Topics

Viva Topics ist ein Modul für das unternehmensweite Organisieren und Bereitstellen von Inhalten und Fachwissen. Mitarbeitende können mit KI-gestützten Tools Unternehmensdaten durchsuchen, erkennen und organisieren.

*„Viva Topics hilft bei der Bewältigung eines wichtigen Geschäftsproblems in vielen Unternehmen – die Bereitstellung der Informationen an Benutzer*innen, wenn sie sie benötigen. Beispielsweise müssen neue Mitarbeiter*innen schnell viele neue Informationen lernen und beim Lesen von Unternehmensinformationen auf Begriffe stoßen, über die sie nichts wissen. Um mehr zu erfahren, muss der Benutzer*innen möglicherweise seine Aktivitäten unterbrechen und wertvolle Zeit damit verbringen, nach Details zu suchen, z. B. nach Informationen über den Begriff, wer in der Organisation Fachexpert*innen ist, und möglicherweise nach Websites und Dokumenten im Zusammenhang mit dem Begriff.*

*Viva Topics verwendet KI, um automatisch nach Themen in Ihrer Organisation zu suchen und diese zu identifizieren. Es werden Informationen über sie zusammengestellt, z. B. eine kurze Beschreibung, Personen, die an dem Thema arbeiten, sowie Websites, Dateien und Seiten, die sich darauf beziehen. Ein Wissensmanager oder Mitwirkender kann die Themeninformationen nach Bedarf aktualisieren. Die Themen stehen Ihren Benutzer*innen zur Verfügung. Dies bedeutet, dass für jede Instanz des Themas, die auf einer modernen SharePoint-Website in Nachrichten und Seiten angezeigt wird, der Text hervorgehoben wird. Benutzer*innen können das Thema auswählen, um mehr darüber in den Themendetails zu erfahren. Themen finden du auch in der SharePoint-Suche."*

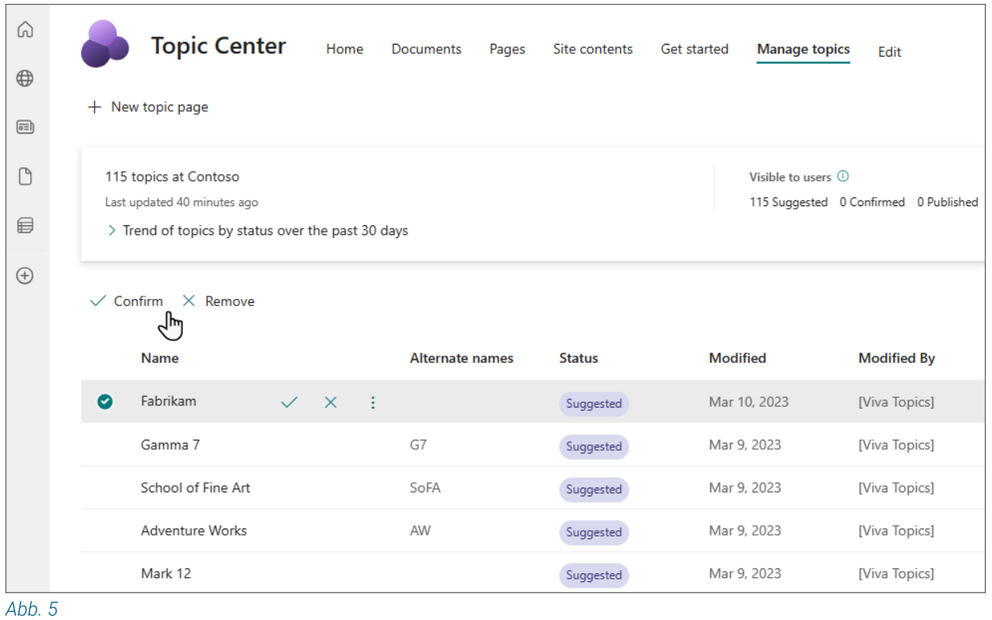


Abb. 5

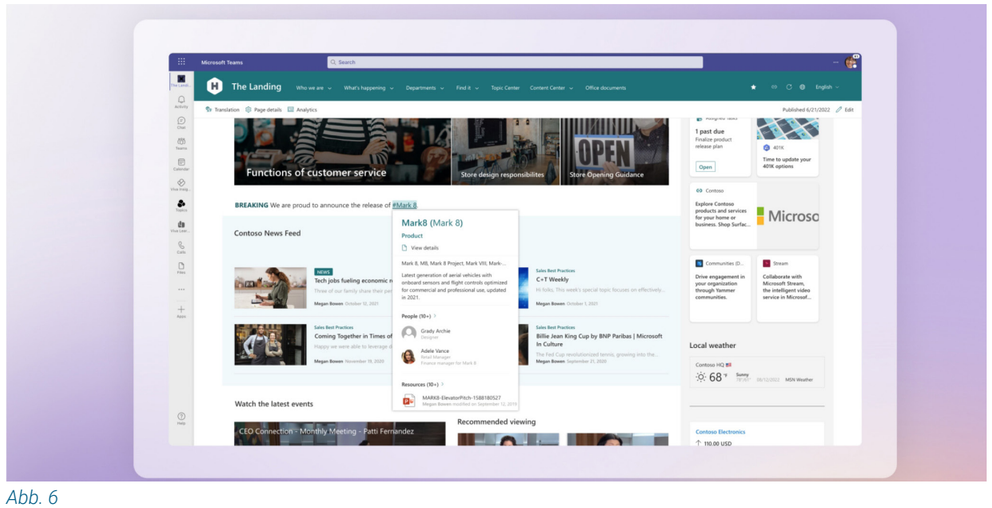


Abb. 6

Über Topics können Nutzer*innen somit Personen, Dokumente und eine Vielzahl weiterer Informationen direkt aus Office-Anwendungen heraussuchen.

Viva Connections

Viva Connections ist ein Modul, dass das Vernetzen der Mitarbeitende und persönliche Kontakte fördern soll.

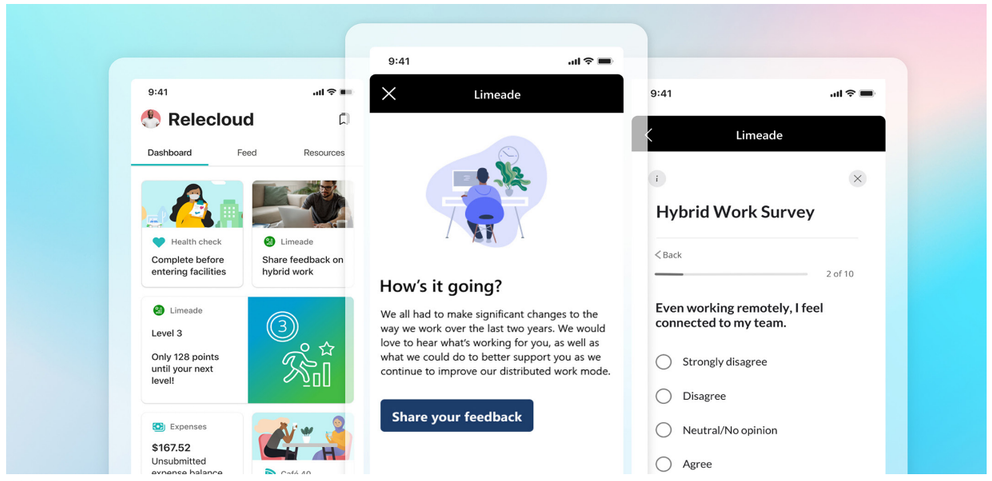


Abb. 7

Viva Goals

Viva Goals soll laut Microsoft eine Zielplanungs- und Managementlösung sein, die Teams auf die strategischen Prioritäten eines Unternehmens ausrichtet und so ergebnisorientiertes und erfolgreiches Arbeiten unterstützt.

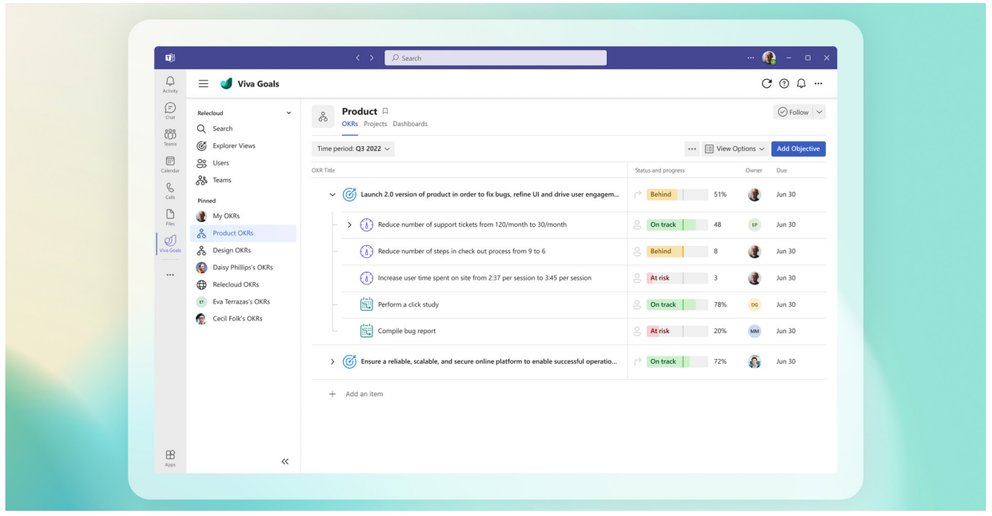


Abb. 8

Delve und MyAnalytics

Delve und MyAnalytics (MyAnalytics wird künftig Teil von Microsoft Viva Insights – s. o. 2.4.2) geben den Nutzerinnen und Nutzern automatisierte Hinweise zur Arbeitsweise und zur Zusammenarbeit mit anderen.

Nutzer*innen erfahren in dem Add-On Delve unter anderem, an welchen Dokumenten sie und auch andere Personen arbeiten. Delve nutzt dabei die von Microsoft Graph gesammelten Daten zu Aktivitäten der Nutzer*innen.

> „Delve zeigt dir eine Mischung aus Inhalten aus allen Microsoft 365. Du siehst sowohl deine eigenen Dokumente als auch die Dokumente, an den deine Kolleginnen und Kollegen arbeiten. Dies sind Dokumente, die in OneDrive für den Arbeitsplatz oder die Schule/Universität oder SharePoint in Microsoft 365 gespeichert oder als Anlagen in E-Mails für dich freigegeben wurden."

Abb. 8

Anhand der ausgewerteten Daten können umfangreiche unzulässige Verhaltens- und Leistungskontrollen der Nutzer*innen durchgeführt werden.

Andere Nutzer*innen bekommen angezeigt, woran jemand zuletzt gearbeitet hat. Daher kann es hier zur Offenlegung von vertraulichen Daten und Informationen kommen. Vorhandene Berechtigungskonzepte können dadurch unterlaufen werden.

Es ist zu beachten, dass beide Module wohl standardmäßig aktiviert sind, wenn sie in der gebuchten Lizenz enthalten sind, ohne dass die einzelnen Nutzer*innen auf die Analyse ihrer Daten hingewiesen werden.

Für Delve kann jede/r Nutzer*in selbst bestimmen, ob ihr/ihm Dokumente angezeigt werden, sofern dies nicht vom Administrator flächendeckend deaktiviert wurde. Zudem können Nutzer*innen Delve auch selbst deaktivieren.

Ob die Dokumente in Delve sicher sind, beantwortet Microsoft auf seiner Webseite selbst wie folgt:

„Ja, Ihre Dokumente sind sicher. Delve ändert niemals irgendwelche Berechtigungen. Nur Sie können Ihre privaten Dokumente in Delve sehen.Andere Personen können auch nicht Ihre privaten Aktivitäten sehen, wie welche Dokumente Sie gelesen haben, welche E-Mails Sie gesendet und empfangen haben oder an welchen Teams-Unterhaltungen Sie sich beteiligt haben. Andere Personen können sehen, dass Sie ein Dokument geändert haben, jedoch nur dann, wenn sie auf dasselbe Dokument zugreifen können.

Beachten Sie, dass Dokumente nicht in Delve gespeichert sind. Wenn Sie Berechtigungen für Dokumente ändern möchten, können Sie dies am Speicherort dieser Dokumente tun, z. B. in OneDrive für den Arbeitsplatz oder die Schule/Universität oder SharePoint in Microsoft 365.

Was Sie in Delve sehen, unterscheidet sich von dem, was für andere Personen angezeigt wird. Sie können Ihre privaten Dokumente und andere Dokumente, auf die Sie Zugriff haben, sehen. Andere Personen können wiederum ihre eigenen Dokumente und die Dokumente anzeigen, auf die sie Zugriff haben."

Durch Nutzer*innen kann Delve wie folgt deaktiviert werden:

So deaktivieren Sie Dokumente in Delve

1. Wechseln Sie in Delve zu **Einstellungen**.

2. Wechseln Sie zu **Featureeinstellungen**, und wählen Sie **Aus** für **Dokumente** aus.

3. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Hinweis: Es kann bis zu einer Woche dauern, bis alle Änderungen wirksam werden.

Was geschieht, wenn andere Personen über Delve verfügen und ich nicht?

Wenn Ihre Organisation Delve verwendet, Sie jedoch nicht über eine Benutzerlizenz verfügen, die Delve umfasst, wird **Delve** nicht im Office 365-App-Startfeld angezeigt.

Andere Delve-Benutzer, also Personen, die über eine Benutzerlizenz verfügen, die Delve umfasst, können Ihre Dokumente in Delve anzeigen, wenn Sie bereits in Office 365 Zugriff darauf haben.

Wenn Sie verhindern möchten, dass Ihre Dokumente auf Ihrer Profilseite in Delve für andere Delve-Benutzer angezeigt werden, können Sie die Anzeige von Dokumenten in Delve deaktivieren. Wenn Sie nicht über Delve verfügen, ist dies über Ihre Seite **Profil** in Office 365 möglich:

1. Um zu Ihrer Seite **Profil** zu wechseln, wählen Sie Ihr Bild in der Office 365-Kopfzeile aus, und klicken Sie dann auf **Über mich**.

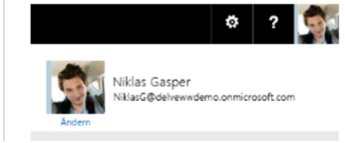


Abb. 9

Yammer

Bei Yammer handelt es sich um ein „soziales Unternehmensnetzwerk".

Die Plattform bietet Funktionen wie Chats, Newsfeed, Gruppenunterhaltungen, fachliche und thematische Foren. Die Nutzer*innen legen ein eigenes Profil an.

Wenn Yammer als Kommunikationsmittel bzw. zum Austausch betrieblicher Informationen genutzt werden soll, sind die internen Berechtigungsstrukturen zwingend auf den Einsatz von Yammer zu übertragen.

Eine Verpflichtung der Mitarbeiter*innen zur Anlegung und Pflege eines Profils wird zudem wohl nicht rechtlich wirksam durchsetzbar bzw. nur auf freiwilliger Basis möglich sein. Soweit die Benutzeraktivitäten ausgewertet werden sollen, ist im Einzelfall zu prüfen, ob eine Einwilligung für diese Datenverarbeitung erforderlich ist.

Graph

Bei Graph handelt es sich um eine Komponente, die im Hintergrund von Microsoft 365 arbeitet. Sie sammelt und vernetzt Daten verschiedener Microsoft 365-Produkte. Es werden nicht nur die Daten, sondern auch die Interaktion der Nutzer*innen mit den Daten und untereinander analysiert, was diese Funktion besonders kritisch macht. Ziel ist eine Art softwarebasierte persönliche Assistenz, die Nutzer*innen bei der Arbeit unterstützt, indem sie auf möglicherweise interessante Dateien und Kontakte hinweist. Dabei werden nur Daten berücksichtigt, für die die jeweiligen Nutzer*innen auch Zugriffsrechte besitzen.

Einfach gesagt „beobachtet" Graph das Tun der Nutzer*innen. Die unterschiedlichen Nutzungen werden als „Signal" von Graph interpretiert und mit Merkmalen versehen in einem Index gespeichert.

Signale können z. B. sein: das Speichern/Ändern/Freigeben einer Datei in SharePoint oder OneDrive, der Versand einer E-Mail, der Eintrag einer Besprechung im Terminkalender, ein Chat in Teams, die Teilnahme an einer Online-Besprechung etc.

Diese Signale bewertet Graph und zieht daraus unterschiedliche Rückschlüsse, wie z. B. wer mit wem besonders häufig kommuniziert oder zusammenarbeitet (welche/r Benutzer*in also für eine/n andere/n Benutzer*innen besonders wichtig ist), welche Dateien besonders wichtig sind, an welchen Tagen Benutzer*innen viel und an welchen sie weniger arbeiten.

All diese „Rückschlüsse", Bewertungen und Informationen aus Graph können auf verschiedene Weise genutzt werden:

- Delve: Zeigt die Dokumente an, die Nutzer*innen zuletzt bzw. mit denen sie am häufigsten gearbeitet haben.
- Web-Anwendungen: In der Rubrik „Entdecken" auf der Homepage von Office 365 oder den Startseiten der Web-Anwendungen werden die zuletzt oder besonders häufig verwendeten Dokumente angezeigt.
- MyAnalytics: Zeigt dem/der Nutzer*in Informationen über sein persönliches Arbeitsverhalten und sein Netzwerk mit anderen Mitarbeitenden an. (MyAnaytics wird künftig Teil von Viva.)
- WorkplaceAnalytics: Zeigt dem Nutzer*innen Informationen über sein persönliches Arbeitsverhalten und sein Netzwerk mit anderen Mitarbeitenden an. (MyAnaytics wird künftig Teil von Viva.)
- andere Programme mit zusätzlicher Schnittstelle.

In folgender Grafik veranschaulicht Microsoft die wesentlichen Dienste und Features:

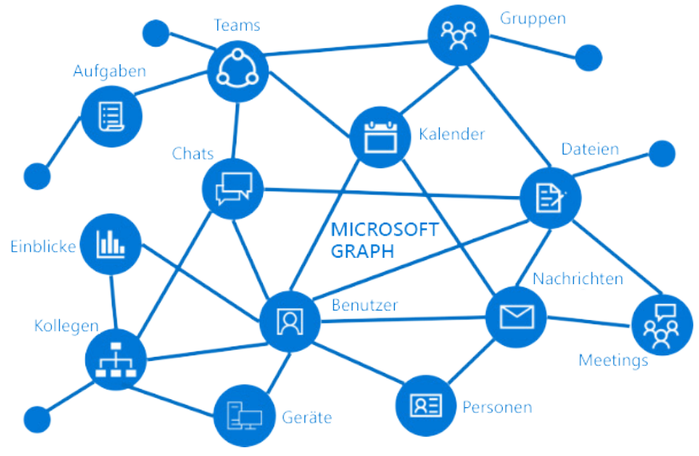


Abb. 10

Entra

Microsoft Entra ist eine neue Produktfamilie von Microsoft. Sie vereint alle Identitäts- und Zugriffsfunktionen von Microsoft, wie Azure Active Directory sowie Cloud Infrastructure Entitlement Management (CIEM) und Decentralized Identity.

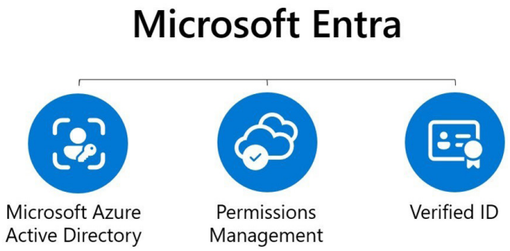


Abb. 11

Azure Active Directory (Azure AD)

Das Azure AD ist ein Cloud-Dienst von Microsoft Azure. Er ermöglicht Administratoren, Identitäten und Zugriffsrechte für Anwender*innen zu verwalten. Es ist also die cloudbasierte Variante des Microsoft Verzeichnisdienstes Active Directory. Administratoren können damit entscheiden, welche Informationen in der Cloud bleiben, wer Informationen verwalten oder verwenden kann, welche Dienste oder Anwendungen auf die Information zugreifen können und welche Endanwender*innen Zugriff darauf haben.

Entra-Berechtigungsverwaltung (CIEM) (Laut Microsoft bald verfügbar)

Die Entra-Berechtigungsverwaltung ist eine neue Lösung, um riskante Berechtigungen in einer Multi-Cloud-Infrastructure erkennen, beseitigen und überwachen zu können. Eine solche CIEM-Lösung soll die stetig zunehmende Zahl von Identitäten, mit denen sich Nutzer*innen an einer Vielzahl von Cloud-Diensten (z.B. Microsoft Azure, Amazon Web Services (AWS) oder der Google Cloud Platform (GCP)) anmelden, beherrscht werden.

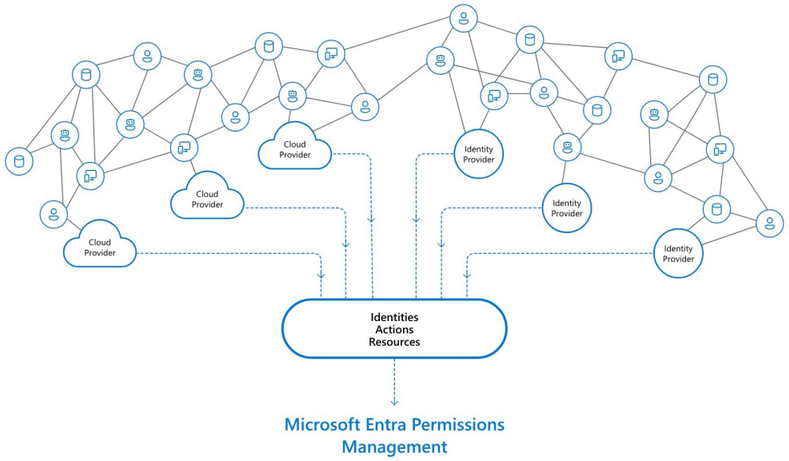


Abb. 12

Entra-ID (vormals "Azure AD-Nachweise")

Entra arbeitet mit verifizierten IDs. Es ist eine Software zur Identitätsprüfung, um Anmeldeinformationen für dezentralisierte Identitäten zu erstellen, auszustellen und zu bestätigen. „Mit verifizierten IDs lassen sich Arbeitsplatzberechtigungen, Qualifikationsnachweise, Zertifizierungen oder sonstige persönliche Identitätsattribute zuverlässig ausstellen und bestätigen."

Die Ausstellung und Prüfung von verifizierten IDs läuft im Drei-Parteien-Verhältnis ab und ähnelt dem von Public- und Private-Key-Verfahren.

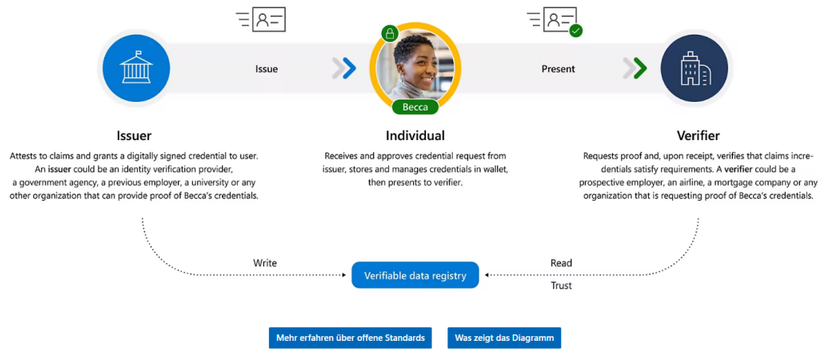


Abb. 13

Connected Experiences

Bei den Connected Experiences (sog. verbundene Dienste) handelt es sich um Online-Mikroservices (wie z. B. Rechtschreibprüfung, Übersetzungstool).

Diese verbundenen Dienste sind teilweise optional und können auf Administratorebene mithilfe der Datenschutz-Zugriffssteuerung für verbundene Dienste oder durch die Richtlinieneinstellung „Verwendung zusätzlicher, optional verbundener Erfahrungen in Office zulassen", verwaltet werden. Einzelne Nutzer*innen können in einer beliebigen Office-Anwendung in den Datenschutzeinstellungen prüfen, welche verbundenen Dienste zur Verfügung stehen.

In erster Linie ist in Bezug auf den Einsatz der Connected Experiences die datenschutzrechtliche Stellung von Microsoft abzugrenzen. Grundsätzlich gibt es einen Auftragsverarbeitungsvertrag, der die Inanspruchnahme von Microsoft als Auftragsverarbeiter regelt. Die Dienste, die im Zusammenhang mit Drittanbietern stehen sind laut den Online-Service-Terms (OST) von Microsoft vom Auftragsverarbeitungsvertrag ausgenommen (z. B. LinkedIn-Integration, Bing-Suche). Die Aktivierung dieser Dienste wird daher nicht empfohlen.

Die Rechtmäßigkeit der einzelnen Funktionen von Connected Experiences muss im Einzelfall für jedes Tool geprüft werden, sofern das Tool nicht deaktiviert wird oder werden soll. Die konkrete Rechtmäßigkeitsprüfung ist Bestandteil der Datenschutz-Folgenabschätzung und bedarf daher keiner weiteren Zusatzaufwände.

Die Connected Experiences werden wie folgt nach der konkreten Funktionsweise unterteilt:

a. Verbundene Dienste, die Inhalte analysieren

Bei den verbundenen Erfahrungen, die Inhalte analysieren, werden der/m Nutzer*in verschiedene Empfehlungen und Vorschläge (z. B. Designempfehlungen, Bearbeitungsvorschläge, Datenerkenntnisse) sowie weitere ähnliche Funktionen bereitgestellt. Die Empfehlungen basieren auf dem analysierten Nutzungsverhalten.

Folgende Funktionalitäten sind beispielhaft von diesen verbundenen Diensten umfasst:

- Designer (Microsoft Word im Web) – Verwenden von Designer für die Erstellung von hochwertigen Dokumenten
- Editor – Ideen in Excel
- Liveuntertitel – Präsentieren in Echtzeit mit automatischen Untertiteln in Powerpoint
- Kartendiagramm – Erstellen eines Kartendiagramms in Excel

b. Verbundene Dienste, die Onlineinhalte herunterladen

Mithilfe der verbundenen Dienste, die Online-Inhalte herunterladen, können Online-Inhalte, wie z. B. Bilder, Vorlagen oder Videos, unmittelbar innerhalb der einzelnen Office-Anwendungen gesucht und heruntergeladen werden.

Hiervon sind beispielhaft folgende Dienste erfasst:

- Cloud-Schriftarten in Office
- Einfügen verschiedener Onlineinhalte in eine Office-Datei (z.B. Symbole in Word, Formular oder Quiz in PowerPoint, Video aus YouTube oder einer anderen Webseite)
- Einfache Recherche für ihr Dokument in Word

c. Weitere verbundene Dienste

Von den weiteren verbundenen Diensten sind folgende sonstige Tools beispielhaft umfasst:

- @Erwähnung – Verwenden von @Erwähnung in Kommentaren, um jemanden für Feedback zu markieren
- Posteingang mit Relevanz (Outlook)
- Zuletzt verwendete Dokumente – Öffnen von Dateien über das Menü „Datei“
- Raumsuche (Outlook) – Steuerung der Raumsuche in Outlook

Eine vollständige Auflistung aller verbundenen Dienste finden Sie auf der Webseite von Microsoft.

Compliance- und Sicherheitstools

Je nach Edition enthält Microsoft 365 einige Compliance- und Sicherheitstools. Speziell für das Datenschutzmanagement bietet Microsoft mit seinem Tool „Priva“ eine Möglichkeit Datenschutzrisiken zu minimieren und auf Betroffenenanfragen automatisiert zu reagieren.

> „Eine Datenschutzmanagement-Lösung, die Datenschutzrisiken proaktiv erkennt und abwehrt, Mitarbeiter*innen zu intelligenten Datenentscheidungen befähigt sowie Anfragen zu Betroffenenrechten in großem Umfang automatisiert und verwaltet.“

04. Rechtliche Bewertung von Microsoft 365

Rechtmäßigkeit der Datenverarbeitung

Die Zulässigkeit der Datenverarbeitung mit Microsoft 365 richtet sich in erster Linie nach den Art. 6, 9 DS-GVO.

Für die Verarbeitung nicht-sensibler personenbezogener Daten mit den Office-Kernanwendungen von Microsoft 365 (Word, Excel, PowerPoint, Outlook) kommen als Rechtsgrundlagen Art. 6 Abs. 1 b) und/oder ggf. c) DS-GVO in Betracht, wenn die Datenverarbeitung zur Vertragserfüllung bzw. zur Erfüllung rechtlicher Verpflichtungen des Verantwortlichen erforderlich ist.

Für die Freigabe und Speicherung personenbezogener Daten in der Cloud allgemein muss das aber nicht gelten, ebenso bei den sonstigen Funktionen von Microsoft 365: Diese sind regelmäßig gerade nicht zur Vertragserfüllung oder Erfüllung rechtlicher Verpflichtungen erforderlich. Entsprechendes gilt für die Datenverarbeitung zur Wahrnehmung einer öffentlichen Aufgabe gemäß Art. 6 Abs. 1 e) DS-GVO.

Für solche Verarbeitungen kommt als Rechtsgrundlage Art. 6 Abs. 1 f) DS-GVO in Betracht, wenn die Verarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen.

Schließlich kann eine Datenverarbeitung auch gemäß Art. 6 Abs. 1 a) i.V.m. Art. 7 DS-GVO auf die Einwilligung der betroffenen Person gestützt werden. Sofern es sich bei dem Betroffenen um eine/n Beschäftigte/n handelt, richtet sich die Zulässigkeit der Datenverarbeitung maßgeblich nach § 26 BDSG oder Art. 6 Abs. 1 f) DS-GVO.

Auftragsverarbeitung und Drittlandübermittlung

Microsoft ist im Wesentlichen als Auftragsverarbeiter des einsetzenden Unternehmens einzustufen. Hiervon ausgenommen sind diejenigen Anwendungen, die von Drittanbietern wie Bing und LinkedIn bereitgestellt werden.

Hierfür bietet Microsoft den Abschluss eines Auftragsverarbeitungsvertrages an, der Teil des sog. Data Processor Agreements (DPA) ist. Dieses DPA beinhaltet auch eine (ziemlich knapp ausgefallene) Beschreibung der technischen und organisatorischen Maßnahmen sowie der EU-Standarddatenschutzklauseln.

Aufgrund der intransparenten Datenverarbeitungen und unzureichend geregelten Kontrollrechte der Auftraggeber sowie einiger Kostenregelungen, steht der Auftragsverarbeitungsvertrag in der Kritik durch die deutschen Aufsichtsbehörden. Der Einsatz von Microsoft 365 ist insoweit daher nicht vollkommen risikofrei.

Als geeignete Garantien zur Rechtfertigung der Datenübermittlung in die USA (Drittland) bietet Microsoft über das DPA den Abschluss von EU-Standarddatenschutzklauseln an. Zumindest hier sind dann z. B. ausreichende Kontrollrechte des Auftraggebers geregelt. Im Sommer 2021 hat die EU-Kommission neue Standardvertragsklauseln herausgegeben.

Es wird aber darauf hingewiesen, dass auch die EU-Standardvertragsklauseln in der Kritik stehen. Der EuGH und die Aufsichtsbehörden haben betont, dass der Abschluss der EU-Standarddatenschutzklauseln die verantwortlichen Unternehmen nicht davon befreit, die jeweiligen Datenübermittlungen konkret zu prüfen und dem Risiko angemessene technische und organisatorische Maßnahmen zu bestimmen und umzusetzen.

Erforderlich ist jedenfalls ein Transfer-Impact-Assessment (TIA), bei dem eine Bewertung der Risiken für die personenbezogenen Daten der Betroffenen erfolgt. Aufgrund der Zugriffsmöglichkeiten der US-amerikanischen Geheimdienste zweifeln aber einige daran, dass eine Datenübermittlung in die USA überhaupt datenschutzkonform erfolgen kann.

Einbeziehung der Mitarbeitendenvertretung

Der Einsatz von Microsoft 365 ist insgesamt auch individual- und kollektivarbeitsrechtlich relevant, da die Software eine technische Einrichtung darstellt, die dazu geeignet ist, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Microsoft speichert für jede mit Microsoft 365 bearbeitete Datei den Bearbeitungszeitpunkt und die Bearbeitungsdauer in einer Log-Datei, die eingesehen werden kann. Daneben werden einige Funktionen angeboten, die konkret dazu geeignet sind, Einblicke in das Arbeitsverhalten der Mitarbeitenden zu erhalten (Viva Insights, Delve). Der Deutsche Gewerkschaftsbund ist der Ansicht, dass Microsoft 365 spätestens seit dem Add-On „Workplace Analytics" (künftig Microsoft Viva Insights) generell zwingend mitbestimmungspflichtig sei.

Laut Microsoft selbst ist aber Microsoft 365 generell zur Leistungs- und Verhaltensüberwachung geeignet (wenn auch nicht spezifisch dazu bestimmt), da Microsoft 365 ein hochgradig anpassbarer Dienst ist, der von einem/einer Datenverantwortlichen potenziell zu einer solchen Verarbeitung verwendet werden kann (Link). Diese Eigenschaft macht den Einsatz von Microsoft Office mitbestimmungspflichtig gemäß § 87 Abs. 1 Nr. 6 BetrVG bzw. des jeweiligen Personalvertretungsgesetzes des Landes.

Wird Microsoft 365 ohne die Einbeziehung der Mitarbeitendenvertretung eingeführt und verwendet, kann diese gegen den Arbeitgeber*in im Wege eines einstweiligen Verfügungsverfahrens eine Unterlassung erzwingen. Sofern Microsoft 365 für alle Geschäftsprozesse verwendet wird, würde dieses Vorgehen zum Arbeitsstillstand und zu erheblichen wirtschaftlichen Ausfällen führen, bis mit den Mitarbeitenden eine Lösung herbeigeführt wird.

05. Handlungsempfehlungen

Um einen weitgehend rechts- und IT-sicheren Einsatz von Microsoft 365 sicherzustellen, sollten folgende Fragen beantwortet bzw. Schritte erwogen werden:

Bestimmung des Prüfgegenstandes

Um feststellen zu können, welche konkreten Maßnahmen zu ergreifen sind, und insbesondere um entscheiden zu können, ob die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich ist, muss genau beschrieben werden, in welcher Edition, Version und mit welchen Konfigurationen Microsoft 365 unter welcher Einsatzumgebung (z.B. ggf. zusätzliche Verwendung von Windows 10) eingesetzt werden soll.

- Wie wird das Projekt lizenzrechtlich umgesetzt?
- Welcher Plan wird gebucht? Welche Module werden angeschafft?
- Welche Rechenzentren wurden ausgewählt?
- Welches Cloud-Modell soll eingesetzt werden (Hybrid-Cloud, public Cloud, private Cloud)?
- Welche Tätigkeiten sollen mit Microsoft 365 abgedeckt werden?
- Sollen Daten nach Art. 9 Abs. 1 DS-GVO verarbeitet werden?
- Sollen Personalangelegenheiten über Microsoft 365 verarbeitet werden?

Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO

Vor Einführung von Microsoft 365 sollte konkret geprüft werden, ob die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO erforderlich ist. Selbst wenn man zu dem Ergebnis kommt, dass keine Datenschutz-Folgenabschätzung durchgeführt werden muss, ist dies zu dokumentieren.

Der Funktionsumfang der meisten Microsoft-Lizenzen erlaubt jedoch den Einsatz datenschutzrechtlich kritischer Anwendungen. Auch wenn solche Anwendungen letztlich nicht produktiv eingesetzt werden sollen, kann wohl alleine schon die Einsatzmöglichkeit die Durchführung einer Datenschutz-Folgenabschätzung bedingen.

Pflichtinformationen nach Art. 13 DS-GVO

Die mit Microsoft 365 stattfindende Datenverarbeitung sollte sich auch in den Pflichtinformationen aller betroffenen Personen wiederfinden. Dafür können eigens für die Nutzung von Microsoft 365 Pflichtinformationen erstellt oder die vorhandenen Informationen ergänzt werden.

Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO

Es sollte nicht vergessen werden, die mit Microsoft 365 zusammenhängenden Datenverarbeitungen im Verzeichnis von Verarbeitungstätigkeiten in den jeweils entsprechenden Verarbeitungstätigkeitskategorien zu ergänzen.

Einwilligungsmanagement

Sofern Verarbeitungstätigkeiten durchgeführt werden sollen, die die Einwilligung der betroffenen Personen erfordern, sind die Voraussetzungen des Art. 4 Nr. 11, 7 DS-GVO, für sensible personenbezogene Daten zusätzlich die des Art. 9 Abs. 2 a) DS-GVO und für Beschäftigtendaten zusätzlich die Voraussetzungen des § 26 Abs. 2 BDSG zu beachten.

Weiterhin sollte die Einholung der Einwilligung im Einklang mit Art. 5 Abs. 2 DS-GVO dokumentiert und aktuell gehalten werden.

Technische und organisatorische Maßnahmen

Von wesentlicher Bedeutung für einen datenschutzkonformen Einsatz von Microsoft 365 ist die Umsetzung adäquater technischer und organisatorischer Maßnahmen. Ganz konkret empfiehlt es sich zunächst zu bestimmen, welche Arten von besonders risikobehafteten personenbezogenen Daten gegebenenfalls vollständig aus der Cloud-Datenhaltung ausgeschlossen werden sollen.

Es ist weiterhin zu empfehlen, die Zugriffsrechte auf Metadaten nach dem „Need-to-know-Prinzip“ auf den erforderlichen Personenkreis zu beschränken, was entsprechend zu dokumentieren ist. Sofern Windows 10 Enterprise als Betriebssystem auf den Computern verwendet wird, sollte das Sicherheitslevel der Telemetrie- und Diagnosedatenübermittlung auf „sicher“ eingestellt werden.

Innerhalb der jeweiligen Microsoft 365-Anwendungen sollte die Einstellung zur Übermittlung von Diagnosedaten auf Administratorebene für alle Nutzer*in auf die möglichst geringste Stufe eingestellt werden. Um zu sehen, welche Diagnosedaten von Windows oder Office an Microsoft übermittelt werden, stellt Microsoft einen „Diagnostic Data Viewer“ zur Verfügung (*Link zum DDV*).

Die Funktion „Customer Experience Improvement Program“ (CEIP; „Verbesserung von Office“) sollte deaktiviert werden, da Microsoft die hierbei übermittelten Daten zu eigenen Zwecken verwendet.

Die als kritisch einzustufenden Anwendungen innerhalb des konkret gebuchten Plans sollten deaktiviert werden, sofern kein dringender Bedarf besteht, diese einzusetzen.

Sofern auch die Connected Experiences aktiviert sind, sind mindestens die Optional Connected Experiences zu deaktivieren („weitere verbundene Dienste“). In einem weiteren Schritt sollten nach einer Bedarfsprüfung aller weiteren nicht genutzten Dienste deaktiviert werden.

Der Auftragsverarbeitungsvertrag mit Microsoft sowie die im DPA enthaltenen EU-Standardvertragsklauseln sollten abgeschlossen werden. Die Ablage der abgeschlossenen Vertrags-Version wird empfohlen, da die aktualisierten Vertragsdokumente regelmäßig nicht automatisch Vertragsbestandteil werden. Ferner sollte ein Transfer Impact Assessment durchgeführt werden.

Es sollte geprüft werden, ob die vorhandenen internen Compliance- und Organisationsinstrumente (z. B. Richtlinien, Anweisungen) sich auf die Datenverarbeitung in Microsoft 365 übertragen lassen oder angepasst werden sollten. Die Mitarbeitenden sollten entsprechend geschult und in Bezug auf den Einsatz von Microsoft 365 sensibilisiert werden.

Schließlich sollten mögliche Rechtsänderungen für die Gültigkeit von Datentransfermechanismen (wie z.B. Standarddatenschutzklauseln) aufgrund künftiger EU-Rechtsprechung oder aufsichtsbehördlicher Praxis im Blick behalten und berücksichtigt werden.

06. Ausblick

Microsoft eröffnet mit seinen Programmen und Technologien eine Vielzahl an Möglichkeiten und Verbesserungen für eine effizientere und vernetztere Zusammenarbeit. Microsoft bietet dazu viele Einstellungsmöglichkeiten, um die Microsoft-Produkte rechtssicher nutzen zu können. Aufgrund seiner überwiegenden Lokalisation in den USA verbleiben insbesondere mit Blick auf den CLOUD-Act und die dazu ergangene Rechtsprechung jedoch weiterhin (datenschutz-) rechtliche Risiken für Unternehmen, die Microsoft 365 umfassend nutzen wollen.

Die EU-Kommission und die USA haben sich im März 2022 zwar auf das „Transatlantic Data Privacy Framework" (TDPF) geeinigt. Das TDPF sieht unter anderem Regelungen zum Zugriff von US-Nachrichtendiensten auf Daten von Europäerinnen und Europäern sowie Vorschriften zu einem Rechtsbehelfsverfahren für Beschwerden von Europäerinnen und Europäern in den USA vor. Das TDPF muss allerdings noch das Verfahren nach § 45 Abs. 3 DS-GVO durchlaufen und stellt damit noch keinen rechtssicheren Rahmen für eine transatlantische Datenübermittlung in die USA dar.

Im August 2022 hat zudem Microsoft eine eigene Stellungnahme zur Datenschutzkonformität von Microsoft 365 und Microsoft Teams abgegeben (*Link zur Stellungnahme*). Darin geht Microsoft u.a. auf die verschiedentlich geäußerten datenschutzrechtlichen Bedenken, insbesondere aus dem öffentlichen Sektor und den Aufsichtsbehörden, bei der Nutzung von Microsoft-Produkten ein.

Ob das Abkommen der EU-Kommission letztlich eine ausreichend rechtssichere Basis für eine rechtskonforme Nutzung von Microsoft 365 darstellen wird und ob auch die Stellungnahme von Microsoft datenschutzrechtlich zutreffend ist, werden am Ende aber möglicherweise wieder die Gerichte feststellen müssen.

07. Abbildungsverzeichnis

08. Quellen- und Linkverzeichnis

Quelle 1 01 Einführung | Festlegungen DSK
Festlegung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24.11.2022 + AG DSK „Microsoft-Onlinedienste" – Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung

Quelle 2 02 Allgemeines zu Microsoft | Datenschutznachtrag von Microsoft| Schrems I-Urteil des EuGH
Angemessenheitsbeschluss der EU-Kommission vom 10.07.2023

Link 1 S. 6 | Zitat Microsoft über Microsoft 365 (zuletzt aufgerufen am 24.11.2023, 14:48 Uhr)
https://www.microsoft.com/de-de/microsoft-365/microsoft-office

Link 2 S. 11 + S. 12 | Zwei Zitate zur Peervergleichen Quelle: Microsoft (zuletzt aufgerufen am 24.11.2023, 15:42 Uhr)
vgl. https://learn.microsoft.com/de-DE/viva/insights/tutorials/comparison-query

Link 3 S. 13 | Zitat Viva Topics ID Quelle: Microsoft Topics (zuletzt aufgerufen am 24.11.2023, 16:01 Uhr)
vgl. https://learn.microsoft.com/de-de/microsoft-365/topics/topic-experiences-overview?view=o365-worldwide

Link 4 S. 15 | Delve und MyAnalytics Zitat 1 Quelle: Microsoft (zuletzt aufgerufen am 24.11.2023, 16:26 Uhr)
https://support.microsoft.com/de-de/office/wie-kann-delve-wissen-was-f%C3%BCr-mich-relevant-ist-048d502e-80a7-4f77-ac5c-f9d81733c385

Link 5 S. 16 | Delve und MyAnalytics Zitat 2 Quelle: Microsoft (zuletzt aufgerufen am 24.11.2023, 16:28 Uhr)
https://support.microsoft.com/de-de/office/sind-meine-dokumente-in-delve-sicher-f5f409a2-37ed-4452-8f61-681e5e1836f3?ui=de-de&rs=de-de&ad=de#bkmk_optout

Link 6 S. 22 | Connectes Experiences (vollständige Auflistung aller Dienste)
Quelle: Microsoft Connectes Experiences (zuletzt aufgerufen am 24.11.2023, 16:46 Uhr)
https://learn.microsoft.com/de-de/deployoffice/privacy/connected-experiences

Link 7 S. 22 | Compliance- und Sicherheitstools Zitat Quelle: Microsoft (zuletzt aufgerufen am 24.11.2023, 16:53 Uhr)
https://www.microsoft.com/de-de/security/business/privacy/microsoft-priva-risk-management?market=de

Link 8 S. 25 | Einbeziehung der Mitarbeitendenvertretung (zuletzt aufgerufen am 30.11.2023, 09:00 Uhr)
https://docs.microsoft.com/de-DE/microsoft-365/compliance/gdpr-dpia-office365

Link 9 S. 27 | Technische und organisatorische Maßnahmen Link zum DDV
Quelle: Microsoft (zuletzt aufgerufen am 24.11.2023, 16:54 Uhr)
https://apps.microsoft.com/store/detail/diagnostic-data-viewer/9N8WTRRSQ8F7?hl=de-de&gl=DE

Link 10 S. 28 | Stellungnahme zur Datenschutzkonformität von Microsoft 365 und Microsoft Teams
Quelle: Microsoft (zuletzt aufgerufen am 24.11.2023, 16:54 Uhr)
https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/08/Microsoft-Statement_Datenschutzkonformitaet-von-Microsoft-365-und-Microsoft-Teams.pdf

Das MORGENSTERN Magazin

the future is yours.

Zum Online-Magazin

MORGENSTERN consecom GmbH
Große Himmelsgasse 1
DE - 67346 Speyer

Telefon
+49 (0) 6232 - 100119 44

E-Mail
contact@morgenstern-privacy.com