

Office 365 bietet eine Vielzahl von Einstellungen und Möglichkeiten zu datenschutzfreundlicher Voreinstellung. Im Umkehrschluss bedeutet dies allerdings auch, dass einige Einstellungen notwendig sind, um die Datensicherheit und die Anforderungen der DSGVO zu erhöhen. Diese Handlungshinweise sollen Ihnen helfen, dies entsprechend zu optimieren.

Dabei hat das Dokument keinen Anspruch auf Vollständigkeit und sichert keinen DSGVO-konformen Betrieb nach Umsetzung. Bei Fragen zum Thema helfen wir Ihnen gerne weiter.

Vertrag und Tarife

Wir beziehen uns in diesem Dokument auf die Office-Abonnements in der Business-Version für Unternehmen.

The image displays four vertical cards representing different Microsoft 365 Business subscription plans. Each card includes the plan name, price per user per month (including VAT), a 'Jetzt kaufen' (Buy now) button, a '1 Monat kostenlos testen' (1 month free trial) link, a list of key features, and a section for included applications and services.

- Microsoft 365 Business Basic:** 4,20 €/Benutzer/Monat. Features include cloud services from Germany, 1 TB cloud storage, and standard security. Includes Word, Excel, PowerPoint, Teams, Outlook, Exchange, OneDrive, and SharePoint.
- Microsoft 365 Business Standard:** 10,50 €/Benutzer/Monat. Features include desktop versions of Office apps, extended security, and webinars. Includes Word, Excel, PowerPoint, Teams, Outlook, Exchange, OneDrive, SharePoint, Access (PC), and Publisher (PC).
- Microsoft 365 Business Premium:** 16,90 €/Benutzer/Monat. Features include desktop versions of Office apps, extended security, and protection from cyber threats. Includes Word, Excel, PowerPoint, Teams, Outlook, Exchange, OneDrive, SharePoint, Access (PC), Publisher (PC), Intune, and Azure Information Protection.
- Microsoft 365 Apps for Business:** 8,80 €/Benutzer/Monat. Features include desktop versions of Office apps, 1 TB cloud storage, and standard security. Includes Word, Excel, PowerPoint, Outlook, OneDrive, Access (PC), and Publisher (PC).

Admin Portale

Hier erhalten Sie eine Übersicht der aktuellen Portale

LINK	Funktion
security.microsoft.com	Microsoft 365 Defender
aad.portal.azure.com	Admin Center Azure Active Directory
endpoint.microsoft.com	Admin Center Endpoint Manager
admin.microsoft.com/sharepoint	Admin Center Sharepoint
admin.exchange.microsoft.com	Admin Center Exchange
admin.teams.microsoft.com	Admin Center Teams
admin.microsoft.com	Admin Center Allgemein

Den Nutzungsumfang der USER legt der Microsoft-365-Administrator fest.

TIPP

- Reduzieren Sie die Anzahl der Administratoren auf ein Minimum, stellen Sie aber eine Vertretung sicher.

Microsoft-365-Tenant

Wenn Sie einen Unternehmens Account angelegt haben, erhalten Sie einen entsprechenden Tenant. Ein Tenant ist vergleichbar mit einer Wohnung in einem Mehrfamilienhaus. Dies ist also Ihr Bereich auf dem Microsoft Server. In der Regel sieht ein solcher Tenant folgendermaßen aus:

„Unternehmen“ onmicrosoft.com

TIPP

- Diesen Tenant können Sie später nicht mehr ändern. Einige Anwendungen nutzen diesen Tenant zu Darstellung nach außen. Hier bietet sich also ein Firmenname oder ähnliches an.

Ihre eigene Domain

Sie haben im Admin Center die Möglichkeit Ihre eigene Domain einzubinden.

Datenspeicherort

Wenn Sie Ihren Tenant mit der deutschen Postanschrift anlegen, hostet Microsoft diesen in einem deutschen Rechenzentrum. Dies stellt aber nicht automatisch sicher, dass auch alle Daten in Deutschland gelagert werden. Im Admin Portal finden Sie eine Aufstellung der Speicherorte Ihres Tenants.

Dienst	Ruhende Daten
Exchange	Europäische Union
SharePoint	Europäische Union
Skype for Business	Europäische Union
Microsoft Teams	Europäische Union

Weiterführende Infos zum Thema erhalten Sie hier:

<https://docs.microsoft.com/de-de/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide>

TIPP

- Bitte beachten Sie das einige andere Anwendungen in den USA lagern.

Benutzer von Microsoft-365 und Gruppen

Im Microsoft Admin-Center können Sie Benutzer anlegen und entsprechende Lizenzen zuweisen. Um einen neuen Benutzer anzulegen, füllen Sie unter „Benutzer/Aktive Benutzer“ zuerst den Abschnitt „Grundlagen“ aus und gelangen dann über den „Weiter“-Button in den Abschnitt „Produktlizenzen“. Um festzulegen, was der jeweilige Nutzer mit der zugewiesenen Lizenz anfangen kann, müssen Sie womöglich auf der Seite herunterscrollen, um den Bereich „Apps“ zum Vorschein zu holen. Darin lassen sich etwa in den Premium-Lizenzen für jeden Nutzer dutzende von standardmäßig freigeschalteten Apps und Funktionsgruppen als Einträge im Azure Active Directory individuell einschränken oder deaktivieren.

In Tenants mit vielen Nutzern kann die Verwaltung von Lizenzen und verfügbaren Apps sehr komplex werden. Die Aufgabe wird leichter, wenn Sie etwa als Inhaber einer Premium-P1- oder -P2-Lizenz für Benutzer mit ähnlichen Aufgaben eine Gruppe im Azure AD einrichten und Lizenzen und Apps für diese Gruppe verwalten. Auf jeden Fall lassen sich aber Apps für einen Nutzer oder eine Gruppe erst dann freischalten, wenn Sie diesem oder dieser zuvor eine Lizenz zugewiesen haben.

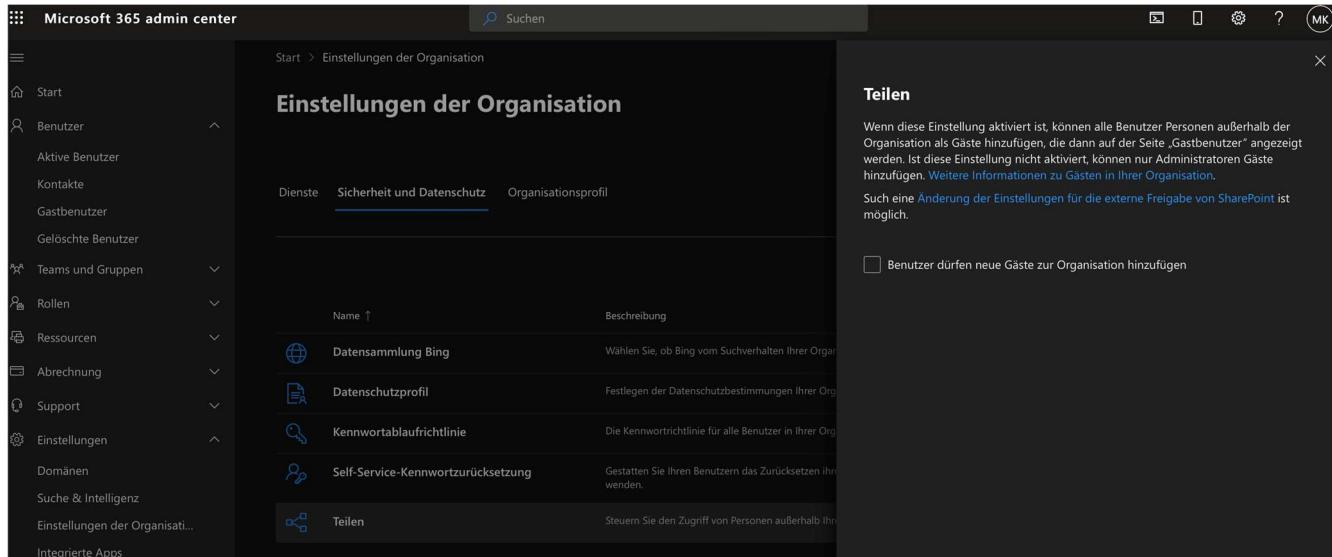
Gastnutzer einsehen und anlegen

Neben den internen Nutzern aus Ihrem Unternehmen, können Sie auch externe Anwender über ihre E-Mail-Adresse als Gastbenutzer in Ihr Tenant einladen. Diese Gastnutzer können dann auch Zugriff auf Ihre Anwendungen wie z.B Teams oder Sharepoint haben. Eine Übersicht Ihrer Gastnutzer finden Sie im Admin Center unter Benutzer.

Verhindern das Gastnutzer von Mitarbeitern angelegt werden

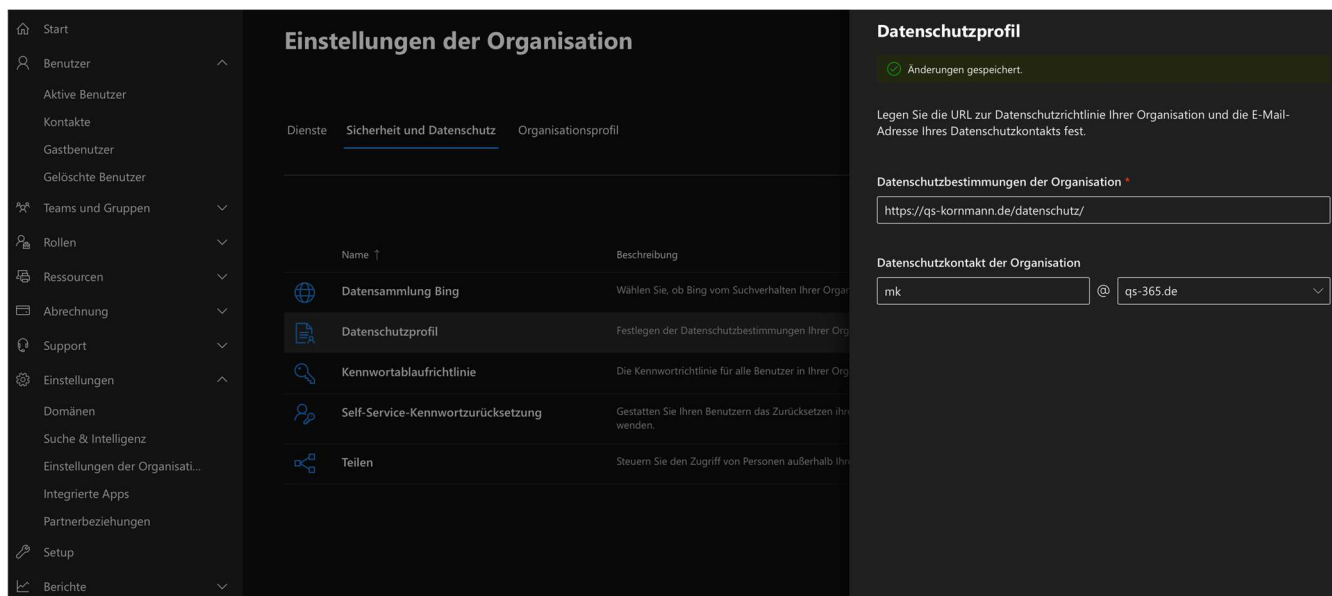
In der Standardkonfiguration kann jeder Mitarbeiter Gäste einladen. Möchte Sie dies verhindern, beachten Sie folgende Punkte

- Öffnen Sie den Admin Center
- Gehen Sie auf Einstellungen
- Gehen Sie auf Einstellungen der Organisation
- Wählen Sie den Reiter Sicherheit und Datenschutz
- Gehen Sie auf Teilen
- Entfernen Sie den Haken bei „Benutzer dürfen Gäste zur Organisation einladen“



Gastnutzer und die DSGVO

Da bei einem Gastnutzer personenbezogene Daten verarbeitet werden, muss jeder Gast Zugriff auf Ihre Datenschutzbestimmung erhalten. Diese werden im Datenschutzprofil verlinkt.



TIPP

- Schaffen Sie klare Regeln zum Umgang mit Gastnutzern
- Prüfen Sie regelmäßig Ihre Gastnutzer und entfernen Sie Benutzer, welche keinen Zugriff mehr benötigen
- Deaktivieren Sie die Funktion, dass jeder Benutzer Gäste einladen kann

SharePoint und OneDrive Sicherheit

Der Teamwork-Webdienst SharePoint Online stellt jedem Benutzer auf OneDrive persönlichen Online-Speicherplatz zur Verfügung. In SharePoint Online und in OneDrive lassen sich Dateien und ganze Ordner für andere Personen freigeben. Diese Personen können ihrer Organisation angehören, müssen es aber nicht. Mit der Standardeinstellung kann man Dateien sogar über einen Link teilen, ohne dass die Identität beim Zugriff geprüft wird. Diese Einstellung sollten Sie im Microsoft 365 Admin Center unter „SharePoint/Organisationseinstellung“ im Reiter „Dienste“ anpassen.

Im SharePoint Admin Center lassen sich dieselben Einstellungen getrennt für SharePoint und OneDrive einstellen. Zuständig dafür ist in der linken Navigationsleiste der Eintrag „Richtlinien/Teilen“. Diese Optionen zu trennen, bietet sich an, wenn Sie zum Beispiel ihre Benutzer darauf beschränken wollen, Daten aus OneDrive nur intern zu teilen, aus SharePoint aber auch das Teilen mit Gästen zu erlauben.

Microsoft 365 admin center

Suchen

Dienste Sicherheit und Datenschutz Organisationsprofil

Name	Beschreibung
Microsoft Graph Data Connect	Verwalten und aktualisieren Ihrer Microsoft Graph...
Microsoft Planner	Wählen Sie aus, ob Ihre Benutzer Pläne und zugew...
Microsoft Search in Bing-Homepage	Anpassen der Seite Bing.com für Ihre angemeldeten...
Microsoft Teams	Verwalten und Aktualisieren Ihrer Microsoft Teams...
Microsoft To Do	Verwalten und Aktualisieren Ihrer To Do-Einstellun...
Microsoft Viva Insights (formerly MyAnalytics)	Verwalten und aktualisieren Sie die Microsoft Viva I...
Microsoft-Kommunikation mit Benutzern	Personen in Ihrer Organisation können E-Mails von...
Microsoft 365 Gruppen	Externes Teilen verwalten.
Modern authentication	Exchange Online Authentifizierungs-Einstellungen f...
Multi-Faktor-Authentifizierung	Verwalten Sie die Einstellungen der Multi-Faktor-Au...
Neues in Office	Verwalten, welche Office Features in den Neuigkeit...
Neuigkeiten	Wählen Sie aus, wie Neuigkeiten über Ihre Organis...
Office im Web	Benutzern das Öffnen von Dateien, die in einem Dr...
Office Scripts	Benutzern das Automatisieren ihrer Aufgaben in Of...
Office-Installationsoptionen	Wählen Sie aus, wie häufig Benutzer Funktions Upd...
Produktivitätsbewertung	Verwalten Sie Datenschutz-Steuerelemente für die P...
SharePoint	Externes Teilen kontrollieren.

SharePoint

Wählen Sie aus, wie Ihre Benutzer SharePoint Websites teilen können, die in Ihrer Organisation erstellt wurden.

Benutzer können teilen mit:

- ☒ Nur Personen in Ihrer Organisation – kein externes Teilen zulässig
- ☐ Nur vorhandene Gäste – Nur Gäste, die bereits im Verzeichnis Ihrer Organisation vorhanden sind.
- ☐ Neue und vorhandene Gäste – Gäste müssen sich anmelden oder einen Prüfcode angeben.
- ☐ Jeder – Nutzer können Dateien und Ordner über Links freigeben, für die keine Anmeldung erforderlich ist

Erweiterte Optionen für externes Teilen

Externes Teilen nach Domäne einschränken, externe Freigabe für nur angegebene Sicherheitsgruppen zulassen, und mehr im Admin Center SharePoint. [Zum Admin Center SharePoint wechseln](#)

TIPP

- Passen Sie die Einstellung Ihrem Unternehmen an.

Datenschutz für Mitarbeiter

Microsoft 365 erfasst allerhand Nutzungsdaten der Benutzer und stellt diese im Microsoft 365 Admin Center, Power BI, Microsoft Graph und im Microsoft Teams Admin Center bereit. So führte der Hersteller im Herbst 2020 den optionalen Dienst „Workplace Analytics“ ein, der unter anderem für jeden Anwender auswertet, an wie vielen Tagen er E-Mails und Yammer-Nachrichten verschickt. Nach zahlreichen Forderungen, dabei den Arbeitnehmer-Datenschutz einzuhalten, stellte Microsoft die ursprünglich wählbare Anonymisierung der verwendeten Daten auf obligatorisch um. Bei älteren Tenants sollten Sie diese Option aber überprüfen. Die Einstellung dazu finden Sie – sofern sie nicht durch ein Update überflüssig geworden ist – im Reiter „Dienste“ unter „Berichte“ in den Organisationseinstellungen.

Microsoft 365 admin center

Suchen

Start > Einstellungen der Organisation

Einstellungen der Organisation

Dienste Sicherheit und Datenschutz Organisationsprofil

Name ↑	Beschreibung
Apps und Dienste im Besitz des Benutzers	Benutzern Zugriff auf die Testversionen von Office 365
Azure Speech Services	Die Verwendung von E-Mails und Dokumenten Ihrer Organisation
Berichte	Verwalten Sie die Datenschutzsteuerung für Admin
Bookings	Auswählen, ob Microsoft Bookings und die zugehörigen
Briefing E-Mail von Microsoft Viva	Personen in Ihrer Organisation das Empfangen von
Calendar	Benutzern das Teilen ihrer Kalender mit Personen von
Cortana	Verwalten Sie den Datenzugriff von Cortana für die Android
Dynamics 365 Applications	Dynamics 365 Applications das Generieren von Erkenntnissen
Dynamics 365 Customer Voice	Zeichnen Sie die Namen der Personen auf, die Umfragen
Dynamics 365 Sales Insights - Analytics	Dynamics 365 das Generieren von Erkenntnissen, basierend auf
Dynamics CRM	Dynamics CRM-Einstellungen Ihrer Organisation verwalten
Mail	Überwachung einrichten, Nachrichten nachverfolgen
Microsoft Edge Websitelisten	Legen Sie für Websites fest, dass sie im Internet Explorer

Berichte

Im Microsoft 365 Admin Center gefundene Berichte enthalten Informationen zu den Nutzungsdaten Ihrer Organisation. Die Daten Ihrer Organisation werden durch vertrauenswürdige Sicherheits- und Datenschutzmaßnahmen in der Cloud verwaltet. Standardmäßig werden in Berichten Benutzerinformationen wie Benutzernamen, Gruppen und Websites ausgeblendet. Sie können sich dazu entscheiden, verborgene Informationen anzuzeigen, wenn Sie dies bevorzugen oder die Richtlinien Ihrer Organisation dies erfordern.

Diese Einstellung gilt für Microsoft 365 Nutzungsberichte in Microsoft 365 Admin Center, Microsoft Graph und Power BI sowie die Verwendungsberichte im Microsoft Teams Admin Center.

☐ Ausgeblendete Benutzer-, Gruppen- und Websitesnamen in allen Berichten anzeigen

Microsoft 365 Verwendungsanalyse

Verwendungsdaten werden analysiert und zum Erstellen von Diagrammen und Grafiken verwendet, damit Sie die Verwendung von Apps und Diensten in Ihrer Organisation besser verstehen. Berichte finden Sie im Microsoft 365 Admin Center und in Power BI. [Informieren Sie sich über die ersten Schritte mit Power BI](#)

☐ Berichtsdaten für Microsoft 365-Verwendungsanalysen für Power BI zur Verfügung stellen

Kalenderzugriff

Exchange-Benutzer können ihren Kalender auch mit Personen außerhalb der Organisation teilen. Das ist problematisch, wenn ein Termin sensible Daten enthält. Zur Vorsorge dagegen können Sie diese Funktion über die Einstellung „Calendar“ in den Organisationseinstellungen im Reiter „Dienste“ unternehmensweit einschränken oder ganz abschalten.

The screenshot shows the Microsoft 365 Admin Center interface. On the left is a navigation pane with categories like 'Benutzer', 'Teams und Gruppen', 'Rollen', 'Ressourcen', 'Abrechnung', 'Support', and 'Einstellungen'. The main area is titled 'Dienste' (Services) and contains a list of services. The 'Calendar' service is highlighted. On the right, a detailed view of the 'Calendar' settings is shown, including a checkbox for 'Externes Teilen' (External sharing) and a section for 'Erweiterte Optionen' (Advanced options).

Name	Beschreibung
Bookings	Auswählen, ob Microsoft Bookings und die zugehörigen Kalender für Ihre Organisation verfügbar sind.
Briefing E-Mail von Microsoft Viva	Personen in Ihrer Organisation das Empfangen von Briefing E-Mails von Microsoft Viva ermöglichen.
Calendar	Benutzern das Teilen ihrer Kalender mit Personen außerhalb Ihrer Organisation gestatten.
Cortana	Verwalten Sie den Datenzugriff von Cortana für die Android-App.
Dynamics 365 Applications	Dynamics 365 Applications das Generieren von Erkenntnissen, basierend auf Ihren Daten.
Dynamics 365 Customer Voice	Zeichnen Sie die Namen der Personen auf, die Umfragen in Dynamics 365 Customer Voice ausfüllen.
Dynamics 365 Sales Insights - Analytics	Dynamics 365 das Generieren von Erkenntnissen, basierend auf Ihren Daten.
Dynamics CRM	Dynamics CRM-Einstellungen Ihrer Organisation verwalten.
Mail	Überwachung einrichten, Nachrichten nachverfolgen.

Calendar

Externes Teilen

☐ Ihren Benutzern das Teilen ihrer Kalender mit Personen außerhalb Ihrer Organisation gestatten, die über Office 365 oder Exchange verfügen.

Erweiterte Optionen

Externe Freigaben auf bestimmte Benutzer anwenden und weitere E-Mail- und Kalender-Einstellungen im Exchange Admin Center verwalten. [Zum Exchange Admin Center wechseln](#)

Spamschutz

Der Spamschutz von Microsoft Exchange Online schützt nicht nur ihre Benutzer vor ungewollten und böswilligen Inhalten, sondern auch ihr Unternehmen vor unbeabsichtigten Aktionen ihrer Benutzer. Ein Beispiel: In den meisten Mailclients, darunter auch Outlook, können Benutzer Regeln zum automatischen Sortieren und Weiterleiten von E-Mails aufstellen. Das führt leicht dazu, dass auch Mails mit vertraulichem Inhalt unbeabsichtigt nach außen weitergeleitet werden. Im letzten Jahr hat Microsoft daher die standardmäßige Spam-Richtlinie für ausgehende Nachrichten so erweitert, dass solche Weiterleitungen nicht mehr möglich sind. Überprüfen Sie einmal ihre Standardeinstellungen im Microsoft 365 Defender Portal unter dem Punkt „Richtlinien und Regeln“ unter „Bedrohungsrichtlinien“ und fügen Sie eigene Regeln passend für ihr Unternehmen hinzu.

Microsoft 365 Defender

Richtlinien und Regeln > Bedrohungsrichtlinien

Bedrohungsrichtlinien

Vorlagenbasierte Richtlinien

- Vordefinierte Sicherheitsrichtlinien** Einfaches Konfigurieren von Schutz durch gleichzeitiges Anwenden aller Richtlinien mithilfe unserer empfohlenen Schutzvorlagen
- Konfigurationsanalyse** Erkennen Sie Probleme in Ihrer aktuellen Richtlinienkonfiguration, um Ihre Sicherheit zu verbessern

Richtlinien

- Antiphishing** Schützen Sie Benutzer vor Phishing-Angriffen und konfigurieren Sie Sicherheitstipps für verdächtige Nachrichten.
- Antispam** Schützen Sie die E-Mail Ihrer Organisation vor Spam, einschließlich der zu ergreifenden Maßnahmen, wenn Spam erkannt wird
- Antischadsoftware** Schützen Sie die E-Mail Ihrer Organisation vor Schadsoftware; mit Maßnahmen und zu benachrichtigenden Personen, wenn Schadsoftware erkannt

Regeln

- Mandantenzulassungsliste-/ -sperr...** Verwalten Sie zugelassene oder blockierte Einträge für Ihre Organisation.
- DKIM** Fügen Sie Ihren Domänen DKIM-Signaturen (DomainKeys Identified Mail) hinzu, damit die Empfänger wissen, dass E-Mails tatsächlich von Ihren Ber...
- Erweiterte Zustellung** Außerkraftsetzungen verwalten für spezielle Systemanwendungsfälle.
- Erweiterte Filterung** Konfigurieren Sie die EOP-Überprüfung (Exchange Online Protection) so, dass sie richtig funktioniert, wenn der MX-Eintrag Ihrer Domäne E-Mail nic...
- Quarantäne-Richtlinien** Anwenden von benutzerdefinierten Regeln auf in Quarantäne befindliche Nachrichten, indem Sie Standard-Quarantäne-Richtlinien verwenden oder

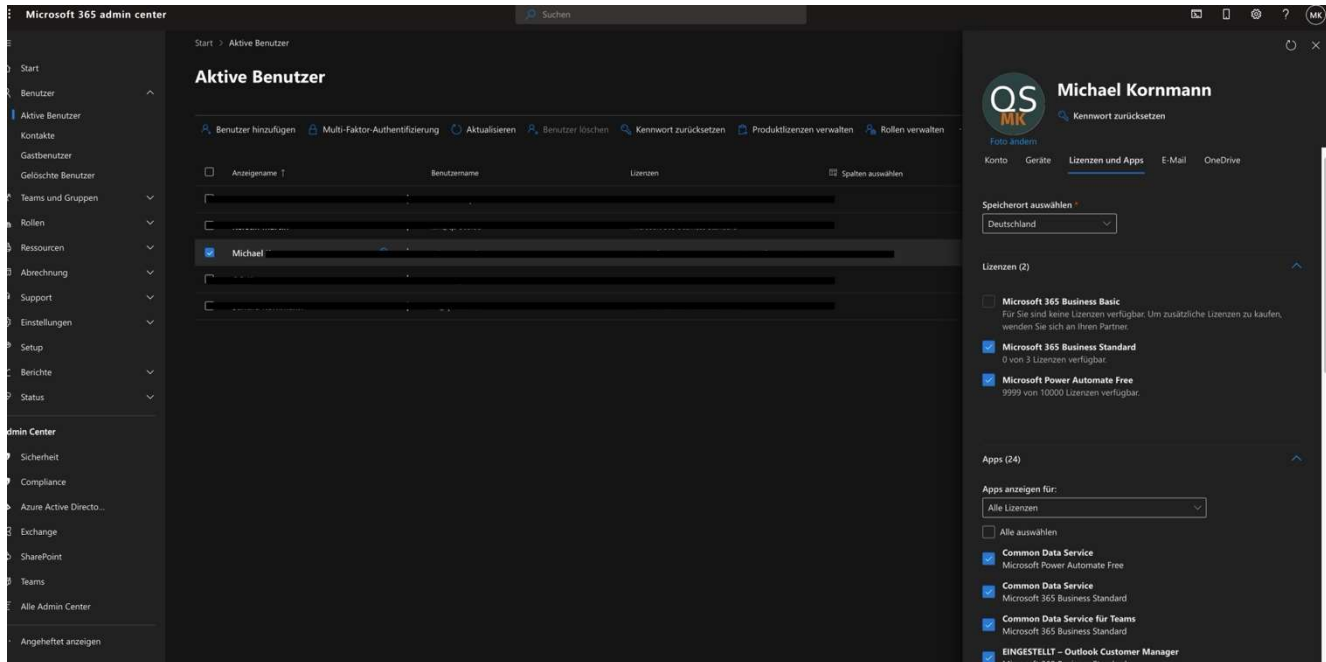
Andere

- Einstellungen für vom Benutzer ge...** Ermöglichen Sie Endbenutzern das Melden von Spam und bösartigen E-Mails zur Überprüfung und Analyse
- Evaluierungsmodus** Konfigurieren Sie Microsoft Defender für Office 365 ohne Ihre Produktionsumgebung zu beeinträchtigen

App Berechtigungen für USER

Sie können jedem USER Rechte für die Nutzung von Anwendungen erteilen oder entziehen.

Bitte passen Sie dies auf Ihr Unternehmen an. Die Funktion finden Sie im Admin Portal unter „aktiver Benutzer“ im Reiter Lizenzen und Apps



TIPP

Deaktivieren Sie folgende Funktionen:

- Whiteboard
- Office im Web
- MyAnalytics
- Power Automate

Weiterführende Informationen:

Weiterführende Informationen und unterstützende Dokumente erhalten Sie unter anderem hier:

https://fragdenstaat.de/anfrage/datenschutzfolgeabschätzungen/644906/anhang/DSFA_und_Anlagen.zip

TIPP

- Beachten Sie Anlage 03 zur Implementierung. Dort finden Sie gute Ansätze und Hinweise

<https://www.rz.uni-wuerzburg.de/dienste/it-recht/it-vertraege/microsoft-365/>

TIPP

- Sehr umfangreich und nützlich, wenn Ihnen der obere LINK keine ausreichenden Infos liefert.