

Informationen zur Verarbeitung personenbezogener Daten bei der Verwendung von Microsoft 365 Produkten („MS 365“)

Mit den folgenden Informationen geben wir Ihnen einen Überblick über die Verarbeitung Ihrer personenbezogenen Daten im Rahmen der Verwendung von Microsoft 365 Produkten gem. Art. 13 und 14 DSGVO geben. Welche Daten im Einzelnen verarbeitet und in welcher Weise diese genutzt werden, richtet sich maßgeblich nach den einzelnen Nutzungsmöglichkeiten und Einsätzen der Anwendungen.

1. Kontaktdaten

Verantwortlicher:	Zuständige Datenschutz-Aufsichtsbehörde:	Datenschutzbeauftragter:
Rhein-Neckar-Verkehr GmbH Möhlstraße 27 68165 Mannheim Tel.: +49 621 46 50 E-Mail: info@rnv-online.de	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden- Württemberg Lautenschlagerstraße 20 70173 Stuttgart Tel.: +49 711 615541-0 E-Mail: poststelle@lfdi.bwl.de	CTM-COM GmbH Marienburgstraße 27 64297 Darmstadt Tel.: +49 154 57605-111 E-Mail: datenschutz@ctm-com.de

2. Allgemeine Information über die Verarbeitung personenbezogener Daten mittels Microsoft 365

Um sowohl einen reibungslosen Betrieb als auch eine unterbrechungsfreie, einfache Kommunikation und Zusammenarbeit sicherzustellen, hat sich unser Unternehmen entschieden, hierfür Microsoft 365 Produkte (**nachfolgend: „MS 365“**) einzusetzen.

Die durch uns durchgeführte Datenverarbeitung mit MS 365 erfolgt auf Servern in Rechenzentren innerhalb der Europäischen Union.

Durch die Bereitstellung und Nutzung von MS 365 können jedoch personenbezogene Daten durch Microsoft in ein Drittland (d. h. außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR)) übermittelt werden, in dem Microsoft oder seine Unterauftragsverarbeiter tätig sind – hier: USA.

Wir haben jedoch geprüft, dass dabei ein angemessenes Datenschutzniveau besteht und die Offenlegung bzw. Übermittlung personenbezogener Daten an Microsoft nur im Einklang mit den gesetzlichen Vorgaben der Art. 44 bis 49 DSGVO erfolgt. Zu diesem Zweck ist Microsoft mit unserem Unternehmen vertragliche Verpflichtungen durch sogenannte Standardschutzklauseln der EU-Kommission eingegangen, die Microsoft zu einer Datenverarbeitung verpflichten, welche dem EU-Datenschutzniveau entspricht.

Da sich Microsoft das Recht vorbehält, Kundendaten zu eigenen legitimen Geschäftszwecken zu nutzen, können wir deren Datenverarbeitung nicht beeinflussen. Unser Unternehmen achtet jedoch bei der

Installation und Administration auf die datenschutzfreundlichen Voreinstellungen und unterbindet die Übertragung von sog. Metadaten, soweit es technisch möglich ist, auf ein absolutes Mindestmaß. (Siehe auch **Punkt 7**)

Für eine weitere Verarbeitung von personenbezogenen Daten, die bspw. durch Besuche auf Microsoft-Webseiten entstehen, haben wir keinen Einfluss in der Administration und übernehmen dafür keine Verantwortung.

Aufgrund des neuen Angemessenheitsbeschlusses mit den USA gibt es ein geringes Risiko für die Rechte und Freiheiten natürlicher Personen. Außerdem werden die Daten an Servern gespeichert, die sich innerhalb der EU befinden.

3. Zwecke und Rechtsgrundlagen für die Datenverarbeitung durch unser Unternehmen

3.1 Genutzte Produkte und zugehörige Verarbeitungszwecke

Unser Unternehmen verarbeitet grundsätzlich nur solche Daten, die für die Erfüllung festgelegter Zwecke im Beschäftigungs- Kunden- Lieferanten – Interessenten oder Bewerberverhältnis etc. notwendig sind.

Konkret nutzen wir folgende Microsoft 365 Produkte zu den angegebenen Zwecken:

- Office (Word, Excel, PowerPoint)
- Microsoft Exchange Online in Verbindung mit Outlook
- Microsoft Teams für Telefon- und Videokonferenzen
- MS Forms (Erstellung von Umfragen und Abstimmungen)
- One Drive (Speicherdienst zum Hosting von Dateien in der Cloud)
- SharePoint (Speicherung, Verarbeitung, Applikationsplattform)
- Azure Active Directory (Single Sign On) <https://learn.microsoft.com/de-de/azure/active-directory/manage-apps/what-is-single-sign-on>
- Microsoft Planer (Aufgabenverwaltung für kleine bis mittlere Teams und Projekte)

Ergänzend hinzu kommen Sicherheitswerkzeuge wie die Defender Produktreihe, Intune als App- und Geräteverwaltungswerkzeug und Whiteboard (digitales Whiteboard). Die vom System erstellten Protokolle, sowie administrative Ereignisse werden zur Fehler-, Support-, Statistik- sowie zu Nachweiszwecken genutzt.

3.2 Rechtsgrundlagen

Wir verarbeiten Ihre personenbezogenen Daten bei der Nutzung von MS 365 unter Verwendung folgender Rechtsgrundlagen:

- **Einwilligung (Art. 6 Abs. 1 S. 1 lit. a. DSGVO)** – Sie haben ihre Einwilligung in die Verarbeitung der Sie betreffenden personenbezogenen Daten für einen spezifischen Zweck oder mehrere bestimmte Zwecke gegeben.

- **Vertragserfüllung und vorvertragliche Anfragen (Art. 6 Abs. 1 S. 1 lit. b. DSGVO)** – Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen (insbesondere auch zur **Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses** auf Grundlage des Arbeitsvertrags gem. § 26 BDSG).
- **Rechtliche Verpflichtung (Art. 6 Abs. 1 S. 1 lit. c. DSGVO)** – Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der unser Unternehmen unterliegt.
- **Berechtigte Interessen (Art. 6 Abs. 1 S. 1 lit. f. DSGVO)** – Die Verarbeitung ist zur Wahrung der berechtigten Interessen unseres Unternehmens oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.
- **Offenlegung an Microsoft jenseits der Auftragsvereinbarung** (Art. 6 Abs. 1 lit. b DSGVO und Art. 49 Abs. 1 lit. c DSGVO) – Vgl. Übersicht der Verarbeitungszwecke durch Microsoft unter **1.1**.

Diese Informationen umfassen nicht die Drittanwendungen und Schnittstellen Dritter, die an die Microsoft 365 Plattform angebunden wurden. Hierfür verweisen wir auf die gesonderten Datenschutzerklärungen innerhalb der nicht zu Microsoft 365 gehörenden Anwendungen. Im **Anhang (A)** sind Services beschrieben, die mittels Microsoft Azure SSO angebunden sind.

3.3 Zwecke für die Datenverarbeitung durch Microsoft

Eine Offenlegung von personenbezogenen Daten an Microsoft erfolgt zu nachstehend aufgelisteten Zwecken. Microsoft handelt hier als eigener Verantwortlicher.

- Abrechnung- und Kontoverwaltung
- Vergütung
- Interne Berichterstattung und Modellierung
- Bekämpfung von Betrug
- Cyberkriminalität oder Cyberangriffen
- Verbesserung der Kernfunktionalität in Bezug auf Barrierefreiheit, Datenschutz oder Energieeffizienz
- Finanzberichterstattung
- Einhaltung gesetzlicher Verpflichtungen

4. Datenkategorien und Kategorien betroffener Personen

4.1 Datenkategorien

Kategorien von Daten: Die übermittelten personenbezogenen Daten, die in E-Mails, Dokumenten und anderen Daten in elektronischer Form im Rahmen der Produkte und Services enthalten sind. Microsoft bestätigt, dass der Kunde je nach Nutzung der Produkte und Services die Möglichkeit hat,

Datenschutz / IT-Sicherheit

personenbezogene Daten aus einer der folgenden Kategorien in die personenbezogenen Daten aufzunehmen:

1. Personenbezogene Basisdaten (z. B. Geburtsort, Straßenname und Hausnummer (Adresse), Postleitzahl, Wohnort, Land der Ansässigkeit, Mobiltelefonnummer, Vorname, Nachname, Initialen, E-Mail-Adresse, Geschlecht, Geburtsdatum) einschließlich der personenbezogenen Basisdaten von Familienmitgliedern und Kindern;
2. Authentifizierungsdaten (z. B. Benutzername, Kennwort oder PIN-Code, Sicherheitsfrage, Audit-Protokoll);
3. Kontaktinformationen (z. B. Adressen, E-Mail-Adressen, Telefonnummern, Social-Media-Kennungen, Notfallkontaktdaten);
4. Eindeutige Identifikationsnummern und Signaturen (z. B. Sozialversicherungsnummer, Bankkontonummer, Pass- und Ausweisnummer, Führerscheinnummer und Kfz-Zulassungsdaten, IP-Adressen, Personalnummer, Studentenummer, Patientenummer, Signatur, eindeutige Kennung bei Tracking-Cookies oder ähnliche Technologien);
5. Pseudonymisierte Kennungen;
6. Finanz- und Versicherungsinformationen (z. B. Versicherungsnummer, Bankkontoname und -nummer, Kreditkartenname und -nummer, Rechnungsnummer, Einkommen, Art der Versicherung, Zahlungsverhalten, Bonität);
7. Geschäftsinformationen (z. B. Kaufverlauf, Sonderangebote, Abonnementinformationen, Zahlungsverlauf);
8. Biometrische Informationen (z. B. DNA, Fingerabdrücke und Iris-Erfassungen);
9. Standortdaten (z. B. Mobilfunk-ID, Geolokalisierungsdaten, Standort bei Beginn/Ende des Anrufs; Standortdaten, die aus der Nutzung von WLAN-Zugriffspunkten abgeleitet werden);
10. Fotos, Videos und Audio;
11. Internetaktivitäten (z. B. Browserverlauf, Suchverlauf, Lesen, Fernsehen, Radiohören);
12. Geräteidentifikation (z. B. IMEI-Nummer, SIM-Kartenummer, MAC-Adresse);
13. Profilierung (z. B. basierend auf beobachteten kriminellen oder antisozialen Verhaltensweisen oder pseudonymisierten Profilen anhand von aufgerufenen URLs, Click-Streams, Surfprotokolle, IP-Adressen, Domänen, installierten Anwendungen oder Profilen basierend auf Marketingpräferenzen);
14. Personal- und Einstellungsdaten (z. B. Angabe des Beschäftigungsstatus, Einstellungsinformationen (wie Lebenslauf, Beschäftigungsverlauf, Ausbildungsverlauf), Stellen- und Positionsdaten einschließlich geleisteter Arbeitsstunden, Beurteilungen und Gehalt, Angaben zur Arbeitserlaubnis, Verfügbarkeit, Beschäftigungsbedingungen, Steuerdetails, Zahlungsdetails, Versicherungsdetails sowie Standort und Unternehmen);
15. Ausbildungsdaten (z. B. Ausbildungsverlauf, aktuelle Ausbildung, Noten und Ergebnisse, höchster Abschluss, Lernbehinderung);
16. Staatsbürgerschafts- und Aufenthaltsinformationen (z. B. Staatsbürgerschaft, Einbürgerungsstatus, Familienstand, Nationalität, Einwanderungsstatus, Passdaten, Angaben zum Aufenthaltsort oder zur Arbeitserlaubnis);
17. Informationen, die zur Erfüllung einer Aufgabe verarbeitet werden, die im öffentlichen Interesse oder in Ausübung der öffentlichen Gewalt ausgeführt wird;
18. Besondere Kategorien von Daten (z. B. ethnische Herkunft, politische Ansichten, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Daten zur Gesundheit, Daten

- über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person oder Daten über strafrechtliche Verurteilungen oder Anklagen); oder
19. Alle anderen in Artikel 4 DSGVO genannten personenbezogenen Daten.

4.2 Kategorien betroffener Personen

Betroffene Personen: Betroffene Personen sind die Vertreter des Kunden und Endnutzer sowie Angestellte, Auftragnehmer, Mitarbeiter und Kunden des Kunden. Zu den betroffenen Personen können auch Personen gehören, die personenbezogene Daten an Nutzer der von Microsoft bereitgestellten Services übermitteln oder Kontakt zu solchen Nutzern aufnehmen möchten. Microsoft bestätigt, dass sich der Kunde je nach Nutzung der Produkte und Services dafür entscheiden kann, personenbezogene Daten von einer der folgenden Arten von betroffenen Personen in die personenbezogenen Daten aufzunehmen:

1. Mitarbeiter, Auftragnehmer und Zeitarbeitnehmer (derzeitige, ehemalige, zukünftige) der Rhein-Neckar-Verkehr GmbH;
2. Angehörige der oben genannten Personen;
3. Partner/Kontaktpersonen der Rhein-Neckar-Verkehr GmbH; (natürliche Personen) oder Mitarbeiter, Auftragnehmer oder Zeitarbeitnehmer von Partnern/Kontaktpersonen (juristische Personen) (derzeitige, ehemalige, zukünftige),
4. Benutzer (z. B. Kunden, , Besucher usw.) und andere betroffene Personen, die Benutzer der Dienstleistungen der rnv sind,
5. Partner, Stakeholder oder einzelne Personen, die aktiv mit den Mitarbeitern der rnv zusammenarbeiten, kommunizieren oder anderweitig interagieren und/oder Kommunikationsmittel wie Anwendungen und Websites verwenden, die vom Kunden bereitgestellt werden;
6. Stakeholder oder einzelne Personen, die passiv mit dem Datenexporteur interagieren (z. B., weil sie Gegenstand einer Untersuchung oder Studie sind oder in Dokumenten oder in Korrespondenz mit dem Datenexporteur erwähnt werden);
7. Minderjährige Personen; oder
8. Berufsgeheimnisträger (z. B. Ärzte, Anwälte, Notare, Kirchenmitarbeiter usw.).

5. Empfänger oder Kategorien von Empfängern der Daten

Empfänger Ihrer personenbezogenen Daten ist bei der Nutzung von unseren eingesetzten Microsoft-Produkten die Microsoft Ireland Operations Ltd., Carmenhall Road, Sandyford, Dublin 18, Ireland, mit ihrem Hauptsitz in den USA (One Microsoft Way Redmond, WA 98052-6399 USA), sowie Personen, mit denen Sie kommunizieren oder zusammenarbeiten.

Weitere Informationen zu den Microsoft-Datenschutzbestimmungen finden Sie unter: <https://privacy.microsoft.com/de-de/privacystatement>

Die Verarbeitung Ihrer personenbezogenen Daten wurde im Rahmen des abgeschlossenen Auftragsvertragsvertrags und der dazugehörigen EU-Standardvertragsklauseln definiert.

Aufgrund des neuen Angemessenheitsbeschlusses mit den USA gibt es ein geringes Risiko für die Rechte und Freiheiten natürlicher Personen. Außerdem werden die Daten an Servern gespeichert, die sich innerhalb der EU befinden.

6. Speicherdauer

Nach Ablauf der vom Gesetzgeber oder den Aufsichtsbehörden erlassenen Aufbewahrungspflichten und Löschfristen werden Ihre Daten grundsätzlich gelöscht. Sofern Daten hiervon nicht betroffen sind, werden sie gelöscht, wenn deren Zweck entfallen ist.

In unserem Unternehmen gelten die Speicherfristen von 90 Tagen.

7. Vorkehrungen im Sinne des Datenschutzes

Die von uns beauftragten Dienstleistungsunternehmen sowie unsere Mitarbeiter*innen sind dazu verpflichtet, die Bestimmungen einzuhalten und Verschwiegenheit hinsichtlich der anwendbaren Datenschutzgesetze zu bewahren. Alle essenziellen technischen und organisatorischen Maßnahmen werden von uns umgesetzt, um daraus resultierend den größtmöglichen Schutz Ihrer von uns verwalteten Daten zu gewährleisten. Darüber hinaus sind wir danach bestrebt, unsere internen Sicherheitsmaßnahmen stetig zu verbessern.

Unser Unternehmen hat bei der Implementierung von Microsoft 365 insbesondere den datenschutzrechtlichen Grundsätzen wie Datenminimierung, privacy by default und privacy by design soweit technisch möglich, Rechnung getragen.

- Die Protokollierung der Verwendung der Dienste von M365 ist aktiviert und pseudonymisiert.
- Eine Funktion zur Produktivitätsbewertung ist nicht aktiviert.
- Die Inventarisierungsfunktion/Telemetrie ist, soweit technisch möglich, abgeschaltet.

8. Ihre Rechte als betroffene Person

Sie haben als betroffene Person dieser Datenverarbeitung folgende Rechte, die Sie gegenüber uns und/oder unseren Dienstleistern wahrnehmen können:

- Recht auf Auskunft,
- Recht auf Berichtigung oder Löschung,
- Recht auf Einschränkung der Verarbeitung,
- Recht auf Widerspruch gegen die Verarbeitung,
- Recht auf Datenübertragbarkeit.

Datenschutz / IT-Sicherheit

Gerne können Sie sich an die E-Mail-Adresse [datenschutz\(at\)ctm-com.de](mailto:datenschutz(at)ctm-com.de) wenden, um Ihre Betroffenenrechte wahrzunehmen.

Sie haben zudem das Recht, sich bei der zuständigen Aufsichtsbehörde (siehe oben) zu beschweren, wenn eine Datenschutzverletzung oder der Verdacht auf eine Datenschutzverletzung vorliegt.

Widerruf von Einwilligungen

Sie haben das Recht jede datenschutzrechtliche Einwilligung, die Sie gegenüber unserem Unternehmen abgegeben haben, jederzeit zu widerrufen. Bei Widerruf der Einwilligung wird die Rechtmäßigkeit der auf ihrer Grundlage bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Gerne können Sie sich an die E-Mail-Adresse [datenschutz\(at\)ctm-com.de](mailto:datenschutz(at)ctm-com.de) um Ihre Einwilligung zu widerrufen.

9. Bereitstellungspflicht

Ohne die die Erstellung eines Accounts ist eine lizenzierte Nutzung von Microsoft 365 nicht möglich.

10. Hinweis

Diese Informationspflicht ist in Ihrer aktuellen Fassung gültig. Durch Änderungen gesetzlicher bzw. behördlicher Vorgaben kann es notwendig werden, diese Information anzupassen. Ebenso werden wir diese Information anpassen, sollten sich in Bezug auf die Verarbeitung personenbezogener Daten bei Microsoft erhebliche Änderungen ergeben.

Das vorliegende Schreiben dient lediglich Ihrer Information. Sie müssen keine Maßnahmen veranlassen. Sollten Sie Fragen, Anmerkungen oder Vorschläge zu diesem Informationsschreiben oder zu unserem Umgang mit dem Datenschutz haben, wenden Sie sich bitte an unseren Datenschutzbeauftragten (**siehe oben**).

11. Weitere Hinweise von und über Microsoft

Einsicht in die Vertragsunterlagen, sowie die von Microsoft eingesetzten Unterauftragnehmer und deren Datenschutzhinweise, können Sie hier nehmen:

- **Auftragsverarbeitungsvertrags als Datenschutznachtrag in Form des "Microsoft Products and Services Data Protection Addendum" (DPA)**
- **Anhang IV der Standardvertragsklauseln der EU-Kommission für verantwortliche und Auftragsverarbeiter**
- **Eingesetzte Unterauftragnehmer**
- **Microsoft Datenschutzbestimmungen**

- **Angemessenheitsbeschluss der EU-Kommission (EU-US Data Privacy Framework)**

Datenschutz / IT-Sicherheit

Anhang (A): Einsatz folgender Produkte von Microsoft 365

Azure Active Directory Premium 1	Microsoft Data Investigations (only E5)
Azure Active Directory Premium 2	Microsoft Defender for Cloud Apps
Azure Information Protection Premium 1	Microsoft 365 Phone System
Azure Information Protection Premium 2 (only E5)	Microsoft Defender for Endpoint
Azure Rights Management	Microsoft 365 Audit Platform
Common Data Service	Microsoft Defender for Identity
Common Data Service for Teams	Microsoft Kaizala Pro
Exchange Online Plan 2	Microsoft Defender for Office 365 Plan 2
Customer Lockbox (only E5)	Microsoft Endpoint DLP (only E5)
Data Classification in Microsoft 365 (only E5)	Microsoft Excel Advanced Analytics (only E5)
Graph Connectors Search with Index (only E5)	Microsoft Information Governance (only E5)
Information Barriers	Microsoft Insider Risk Management (only E5)
Information Protection for Office 365 Premium (only E5)	Microsoft ML-Based Classification (only E5)
Information Protection for Office 365 – Standard	Microsoft Records Management (only E5)
Microsoft 365 Advanced Auditing	Microsoft Forms
Microsoft 365 Apps for Enterprise	Microsoft Intune
Microsoft Azure Multi-Factor Authentication	Microsoft Planner
Microsoft 365 Defender	Microsoft StaffHub
Microsoft Bookings	Microsoft Stream for Office 365 E3
Microsoft Customer Key (only E5)	Microsoft Teams
Office 365 Privileged Access Management (only E5)	Office 365 SafeDocs
Power Apps for Office 365	Office for the Web
Power Automate for Office 365	Office 365 Advanced eDiscovery (only E5)
PowerBI Pro (only E5)	Project for Office (Plan E3)
SharePoint Plan 2	Visio Plan 2
Universal Print	Whiteboard
Windows 10/11 Enterprise	Windows Update for Business Deployment Service
Yammer Enterprise	Insights by MyAnalytics
Microsoft 365 Audio Conferencing	Power Virtual Agents for Office 365
Microsoft 365 Communication Compliance	To-Do (Plan 3)
Microsoft Communications DLP	Viva Learning Seeded
Microsoft MyAnalytics (Full)	Premium Encryption in Office 365
Office 365 Cloud App Security	Viva Engage Core
Windows Autopatch	

Datenschutz / IT-Sicherheit

Anhang (B) Übersicht zu den Datenflüssen der eingesetzten Dienste

Dienst oder Software	Beschreibung des Produktes oder des Onlinedienstes	Weiterführende Informationen oder Hilfen	Maßnahmen bzw. Kontrollmöglichkeiten
Windows 10 Enterprise	Betriebssystem	Windows 10, Version 1909, und Windows 10, Version 1903 – erforderliche Diagnoseereignisse und -felder (Windows 10) - Windows Privacy Microsoft Docs	Datensparsames Level für Diagnosedaten festgelegt. Übersicht über die Diagnosedatenanzeige (Windows 10) - Windows Privacy Microsoft Docs
Microsoft Defender Antivirus	Virenschutz	Datenspeicherung und Datenschutz von Microsoft Defender for Endpoint Microsoft Docs	Als Basisschutz steht der Anti-Mailware-Schutz von Microsoft zur Verfügung.
Microsoft Edge	Browser	Dokumentation für Microsoft Edge - Microsoft Edge Development Microsoft Docs	Alternative Browser wie Mozilla Firefox oder Google Chrome. Ferner dieses Whitepaper zum Microsoft Edge-Datenschutz - Microsoft Edge Development Microsoft Docs
Office Addin Store	Erweiterungen für Microsoft Office	Plattformübersicht für Office Add-Ins - Office Add-ins Microsoft Docs	Deaktiviert.
Microsoft 365 App for Enterprise (Microsoft Office Client)	Desktopanwendungen von Office	Wesentliche Dienste für Office - Deploy Office Microsoft Docs Für Office erforderliche Diagnosedaten - Deploy Office Microsoft Docs Optionale Diagnosedaten für Office - Deploy Office Microsoft Docs	Datensparsames Level für Diagnosedaten festgelegt. Verwenden des Diagnosedaten-Viewers mit Office - Office-Support (microsoft.com)
Office Mobile App	Office Anwendungen für Smartphones	Wesentliche Dienste für Office - Deploy Office Microsoft Docs Für Office erforderliche Diagnosedaten - Deploy Office Microsoft Docs Optionale Diagnosedaten für Office - Deploy Office Microsoft Docs	Datensparsames Level für Diagnosedaten festgelegt. Verwenden des Diagnosedaten-Viewers mit Office - Office-Support (microsoft.com)
Office for the web	Webanwendungen für Microsoft Office	Optionale Diagnosedaten für Office - Deploy Office Microsoft Docs	Optionale Dienste aktiviert.
Office - Verbundene Erfahrungen	Office besteht aus Clientsoftware-Anwendungen und	Für Office erforderliche Dienstdaten - Deploy Office Microsoft Docs	Die Verbundenen Erfahrungen sind aktiv.

Datenschutz / IT-Sicherheit

	verbundenen Erfahrungen, die es Ihnen ermöglichen, effektiver zu erstellen, zu kommunizieren und zusammenzuarbeiten.		
Office - Optional Verbundene Erfahrungen	Dienste außerhalb des Angebotes Microsoft 365, etwa Dienste von Bing oder LinkedIn.	Für Office erforderliche Dienstdaten - Deploy Office Microsoft Docs	Separate Freischaltung erforderlich.
Teams Desktopclient	Client für Teams	Erforderliche Desktop-Client-Diagnosedaten für Microsoft Teams - Microsoft Teams Microsoft Docs	Hier sind die Microsoft Standardeinstellungen aktiv.
Teams mobiler Client	Mobiler Client für Teams	Erforderliche mobile Diagnosedaten für Microsoft Teams - Microsoft Teams Microsoft Docs	Hier sind die Microsoft Standardeinstellungen aktiv.
GIPHY und URL Preview-Dienst in Teams	Optionale Dienste in Teams sind derzeit deaktiviert.	Optionale verbundene Erfahrungen in Teams - Microsoft Teams Microsoft Docs	Aktiviert.
Forms	Umfragen, Quizze und Abstimmungen erstellen und die Ergebnisse bequem in Echtzeit anzeigen.	Microsoft Forms Hilfe & Lernen - Microsoft-Support	In Verantwortung der Anwender*innen.
Lists	Ermöglicht Benutzern das Erstellen, Freigeben und Nachverfolgen von Daten in Listen.	Hilfe & Lernen zu Microsoft Listen - Microsoft-Support	In Verantwortung der Anwender*innen.
OneDrive	Ihre Dateien an einem zentralen Ort speichern, teilen und darauf zugreifen.	OneDrive-Hilfe und -Learning - Microsoft-Support	Feedbackmöglichkeit aktiviert. Anonymes Teilen deaktiviert.
Planner	Pläne erstellen, Aufgaben organisieren und zuweisen, Dateien teilen und sich über den aktuellen Status informieren lassen.	Planner-Hilfe und -Learning - Microsoft-Support	In Verantwortung der Anwender*innen.
Project	Projektpläne entwickeln, Aufgaben zuweisen, Status	Project-Hilfe und -Learning - Microsoft-Support	Datensparsames Level für Diagnosedaten festgelegt.

Datenschutz / IT-Sicherheit

	verfolgen und Budgets verwalten.		Optionale Dienste aktiviert.
Stream	Videos von Kursen, Besprechungen, Präsentationen und Schulungssitzungen teilen.	Berechtigungen und Datenschutz in Microsoft Stream - Microsoft Stream Microsoft Docs	In Verantwortung der Anwender*innen.
Teams	Der anpassbare, chatbasierte Teamarbeitsbereich in Office 365.	Microsoft Teams – Datenschutz - Microsoft Teams Microsoft Docs	Optionale Dienste und Apps teilweise aktiviert. Nur beschränkt bereitgestellte Funktionalität.
To Do	Behalten Sie den Überblick über Ihre Aufgaben an einem Ort mit Informationen, die Ihnen helfen, gemeinsam zu sammeln, Prioritäten zu setzen und mehr zu erreichen.	To Do-Hilfe und -Learning - Microsoft-Support	In Verantwortung der Anwender*innen.
Visio	Komplexe Informationen visuell vereinfachen und vermitteln.	Visio-Hilfe und -Learning - Microsoft-Support	Datensparsames Level für Diagnosedaten festgelegt. Optionale Dienste aktiviert.
Whiteboard	An einem für Stift-, Touch- und Tastatureingabe entwickelten Freihandzeichenbereich gemeinsam Ideen entwickeln und zusammenarbeiten.	Datenschutzeinstellungen in Microsoft Whiteboard - Office-Support	Optionale Erfahrungen und Diagnosedaten sind zentral aktiviert.

<https://support.microsoft.com/de-de/office/verwenden-des-diagnosedaten-viewers-mit-office-cf761ce9-d805-4c60-a339-4e07f3182855>