

Datenschutzhinweise bei der Nutzung von Microsoft 365 Produkten („MS 365“)

Verantwortlichkeiten

CTM-COM GmbH
Marienburgstraße 27
64297 Darmstadt
Deutschland
Telefon: +49 6151 3942–72
E-Mail: datenschutz@ctm-com.de

Kontakt Daten des Datenschutzbeauftragten

CTM-COM GmbH
Marienburgstr. 27
64297 Darmstadt
Deutschland
Telefon: +49 6151 394272
E-Mail: datenschutz@ctm-com.de

Kurzbeschreibung

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.

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.

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.

Zweck der Datenverarbeitung

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, One Note)
- Microsoft Exchange Online in Verbindung mit Outlook
- Microsoft Teams für Telefon- und Videokonferenzen
- MS Forms (Erstellung von Umfragen und Abstimmungen)
- SharePoint (Speicherung, Verarbeitung, Applikationsplattform)
- Azure Active Directory
- Windows 10/11 Enterprise
- Microsoft Search
- Office for the Web
- Microsoft Edge
- Microsoft Whiteboard
- Microsoft Planner
- Microsoft To Do

Die vom System erstellten Protokolle, sowie administrative Ereignisse werden zur Fehler-, Support-, Statistik- sowie zu Nachweiszwecken genutzt.

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

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 anonymisiert.
- Eine Funktion zur Produktivitätsbewertung ist nicht aktiviert.
- Die Inventarisierungsfunktion/Telemetrie ist, soweit technisch möglich, abgeschaltet.

Rechtsgrundlage

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)

Diese Informationen umfassen nicht die Drittapplikationen 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 Applikationen.

Datenquellen

Jeweiliger Betroffener

Datenkategorien

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) des Kunden;
2. Angehörige der oben genannten Personen;
3. Partner/Kontaktpersonen des Kunden (natürliche Personen) oder Mitarbeiter, Auftragnehmer oder Zeitarbeitnehmer von Partnern/Kontaktpersonen (juristische Personen) (derzeitige, ehemalige, zukünftige),
4. Benutzer (z. B. Kunden, Geschäftspartner, Besucher usw.) und andere betroffene Personen, die Benutzer der Dienstleistungen des Kunden sind,
5. Partner, Stakeholder oder einzelne Personen, die aktiv mit den Mitarbeitern des Kunden 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.).

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, 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-Kartennummer, 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.

Regelfristen für die Löschung

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 Speicherfristen von 90 - 180 Tage.

Erfordernis

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

Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

Empfänger Ihrer personenbezogenen Daten ist bei der Nutzung von unseren eingesetzten Microsoft-Produkten die Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Park, Leopardstown, 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 Auftragsverarbeitungsvertrags und der dazugehörigen EU-Standardvertragsklauseln definiert.

Absicht der Übermittlung an ein Drittland oder internationale Organisation

Es erfolgt eine Unterauftragsverarbeitung (Unterauftragnehmer des eingesetzten Auftragsverarbeiters) in einem (oder mehreren) datenschutzrechtlichen Drittland (Drittländern): USA

Angemessenheitsbeschluss der EU Kommission

Kein Angemessenheitsbeschluss der EU Kommission

Recht auf Auskunft

Sie haben das Recht auf Auskunft über die von uns zu Ihrer Person verarbeiteten personenbezogenen Daten. Bei einer Auskunftsanfrage, die nicht schriftlich erfolgt, bitten wir um Verständnis dafür, dass wir dann ggf. Nachweise von Ihnen verlangen, die belegen, dass Sie die Person sind, für die Sie sich ausgeben.

Außerdem stehen Ihnen folgende weitere Rechte zu, die Sie uns und/oder unseren Dienstleistern gegenüber wahrnehmen können:

- *Recht auf Berichtigung oder Löschung,*
- *Recht auf Einschränkung der Verarbeitung,*
- *Recht auf Widerspruch gegen die Verarbeitung,*
- *Recht auf Datenübertragbarkeit.,*
- *Recht auf Widerruf* jeder datenschutzrechtlichen Einwilligung, die Sie uns gegenüber abgegeben haben. Der Widerruf kann jederzeit an die zuvor genannte Kontaktmöglichkeit erfolgen. Bei Widerruf der Einwilligung wird die Rechtmäßigkeit, der auf ihrer Grundlage bis zum Widerruf erfolgten Verarbeitung, nicht berührt.

Gerne können Sie sich über die zuvor genannten Kontaktmöglichkeiten an uns wenden, um Ihre Betroffenenrechte wahrzunehmen.

Recht auf Beschwerde bei einer Aufsichtsbehörde

Es besteht darüber hinaus das *Recht auf Beschwerde bei einer Aufsichtsbehörde*, wenn Sie der Ansicht sind oder der Verdacht besteht, dass die Verarbeitung der Sie betreffenden personenbezogenen Daten gegen datenschutzrechtliche Bestimmungen verstößt.

Kontaktdaten der für unser Unternehmen zuständigen Aufsichtsbehörde:

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit

E-Mail: poststelle@datenschutz.hessen.de