Datenschutzinformationen zur Speicherung und Verarbeitung von externen personenbezogenen Daten in Microsoft 365

Verantwortliche Stelle für die Bereitstellung des Dienstes Microsoft 365 (M365, vormals Office365) ist die:

Tobias Lange Unternehmensberatung
Berner Heerweg 246, 22159 Hamburg
E-Mail: info@tl-datenschutz.de

Die verantwortliche Stelle hat mit der

Microsoft Irland Operations LTD
One Microsoft Place
South county Business Park
Leopardstwon, Dublin 18
D18 P521 Irlanda
(nachstehend Microsoft oder MS)

einen Vertrag über Standarddatenschutzklauseln abgeschlossen, der den Vorgaben der EU entspricht. Microsoft ist Auftragsverarbeiter für die verantwortliche Stelle und stellt die technischen Dienste für M365 zur Verfügung.

Soweit die verantwortliche Stelle M365 oder eine Zusammenarbeit als Auftragsverarbeiter im Sinne des Art. 28 DS-GVO dritten Personen oder Organisationen zur Verfügung stellt, gilt, soweit nicht explizit anderes vereinbart ist, der standardisierte Auftrags-verarbeitungsvertrag (AVV) der verantwortlichen Stelle als vereinbart, welcher auf der Webseite der verantwortlichen Stelle, auf der Unterseite Datenschutzerklärung, jederzeit in aktueller Form abgerufen werden kann.

Für eine Zusammenarbeit über den Dienst MS-Teams innerhalb der Anwendung M365 wird zusätzlich auf die Datenschutzinformationen zur Zusammenarbeit in MS-Teams verwiesen.

Für Personen, welche von einer Speicherung oder Verarbeitung ihrer personenbezogenen Daten mit M365 betroffen sind, auch unabhängig einer Einbindung in die M365 Zusammenarbeit, gelten grundsätzlich alle bestehende Datenschutzrechte nach Kapitel 3 der DS-GVO, insbesondere das Recht auf Auskunft und ein Recht auf Löschung personenbezogener Daten, wenn dieses durch gesetzliche Bestimmungen nicht beschränkt ist. Bezüglich aller Rechte betroffener Personen wird auf die allgemeine Datenschutzinformation für Kunden und Geschäftspartner der verantwortlichen Stelle verwiesen.

In M365 werden grundsätzlich zwei Arten von Daten verarbeiten:

- Inhaltsdaten
- Telemetriedaten

Inhaltsdaten sind alle Dokumente, Dateien, Bilder oder Daten (Zum Beispiel Chat-Verläufe), gleich welcher Art oder welches Formats, die in M365 gespeichert oder mit einem zu diesem Softwarepaket gehörenden Dienst verarbeitet werden. Inhaltsdaten sind in M365 grundsätzlich verschlüsselt und nur zugriffsberechtigten Personen in unverschlüsselter Form zugänglich.

Unter Telemetriedaten sind die Speicherung und Verarbeitung von Daten über die Art, die Zeit, die Dauer, die genutzten Geräte, die Software, die IP-Adressen und die Teilnehmer (Benutzernamen) in Bezug auf eine genutzte Anwendung aus M365 zu verstehen. Diese Daten sind, um die technische Durchführung zu ermöglichen, grundsätzlich unverschlüsselt. Sie sind für Microsoft einsehbar und können durch Microsoft, soweit sie für die verantwortliche Stelle nicht selbst abrufbar sind, auf Verlangen dieser, vollständig an diese herausgegeben werden.

In M365 sind alle inhaltlichen Daten grundsätzlich verschlüsselt. Zugriff haben nur die für die Zusammenarbeit berechtigten Personen. Dritte Personen, insbesondere auch Microsoft selbst, haben keinen Zugriff auf inhaltliche Daten noch eine Möglichkeit der Entschlüsselung der Daten. Namensdaten, Nutzernamen und Telemetriedaten sind regelmäßig unverschlüsselt, um die technische Funktionalität der Anwendung M365 herstellen zu können. Als Logfiles archivierte Telemetriedaten sind verschlüsselt und nur berechtigten Personen zugängig.

Microsoft ist ein US-amerikanisches Unternehmen. Zwischen den USA und der EU wurde Ende 2022 ein Datenschutzabkommen geschlossen, welches die Schutzrechte von EU-Bürgern bzgl. der Speicherung und Verarbeitung ihrer Daten regelt und ein angemessenes, der DS-GVO entsprechendes Datenschutzniveau, sicherstellen soll. Grundsätzlich

kann von Microsoft verlangt werden, dass zur Strafverfolgung besonders schwerer Delikte personenbezogene Daten an US-Behörden übermittelt werden, ohne dass betroffene Personen hierüber informiert werden. In diesem Zusammen-hang sei erwähnt, dass die Ermittlung als auch Prävention von bzw. vor Straftaten elementarer Bestandteil der Ordnung eines jeden demokratischen Rechtstaats sind. In Deutschland ist dieses in der StPO §§ 100a ff. geregelt. Hiernach ist es den Staatsanwaltschaften, die in Deutschland nicht unabhängig sind, erlaubt, ggf. sogar über kurze Zeiträume ohne richterlichen Beschluss, Daten von Unternehmen der Privatwirtschaft zu erhalten und zu verarbeiten. Dieses auch ohne eine Mitteilung an die betroffenen Personen zu tätigen, um Ermittlungs-ergebnisse nicht zu gefährden. Insbesondere dürfen auch technische Maßnahmen zur Überwachung von Datenverkehr oder deren Ausspähung eingesetzt und Unternehmen der Privatwirtschaft zur Mithilfe hierbei verpflichtet werden. Somit herrscht in Deutschland eine andere Art der strafrechtlichen Datenerhebung und Verarbeitung als in den USA, jedoch, in der Gesamtschau, ein vergleichbares Datenschutzniveau aus Sicht betroffener Personen.

Die verantwortliche Stelle bewahrt inhaltliche Informationen mit Personenbezug nur so lange auf, wie ein Zweck für die Speicherung und Verarbeitung vorliegt. Sofern ein Zweck nicht mehr vorliegt, werden die entsprechenden Daten final gelöscht oder für eine gesetzlich vorgeschriebene Aufbewahrung, sofern diese Pflicht besteht, archiviert. Darüber hinaus gelten folgende abweichende Aufbewahrungsfristen für Inhalte:

- Chat- oder Kanalverläufe in MS-Teams werden nach spätestens 12 Monaten automatisiert gelöscht.
- Kalendereinträge werden spätestens 12 Monate nach Ablauf automatisiert gelöscht.
- Yammer Beiträge werden nach 12 Monaten automatisiert gelöscht.
- M365 Gruppen werden nach 12 Monaten Inaktivität automatisiert gelöscht.
- Öffentliche Exchange-Ordner werden spätestens nach 6 Monaten automatisiert gelöscht.
- E-Mails, soweit diese Kunden-korrespondenz darstellen (Empfang wie Versand), werden 6 Jahre aufbewahrt.
- E-Mails, soweit sie nicht unter Kundenkorrespondenz fallen, werden spätestens nach 12 Monaten automatisiert gelöscht.

Die vorgenannten Aufbewahrungsfristen, sofernnicht gesetzlich vorgeschrieben, bestehen zur Aufklärung von Missbrauch und Datenpannen sowie zur Abwehr von etwaigen Rechtsansprüchen. Rechtsgrundlage ist ein berechtigtes Interesse der verantwortlichen Stelle gem. Art. 6 Abs. 1 lit. f.) DS-GVO.

Telemetriedaten oder Nutzerinformationen, welche technisch mit inhaltlichen Daten verbunden sind (zum Beispiel der Besitzer einer Datei oder Zugriffsrechte), werden folgerichtig und technisch nicht anders darstellbar, mit den Inhalten bis zur finalen Löschung dieser aufbewahrt.

Neben mit Inhalten verbundenen technischen Daten werden Telemetriedaten zur Nutzung von Anwendungen und Geräten erhoben. Die Nutzung von Anwendungen und Geräten, insbesondere zur Zusammenarbeit, kann über drei Wege erfolgen:

1. Externe Nutzer*innen erhalten einen Benutzer-namen von der verantwortlichen Stelle unter einer Domain der verantwortlichen Stelle. Sie haben dann den Status „Mitglied“.
2. Externe Nutzer*innen werden über ihre eigenen E-Mailadressen zu einer Anwendung eingeladen. Sie haben dann den Status „Gast“.
3. Externe Nutzer*innen werden ohne Benutzer-namen durch sichere Links an der Zusammenarbeit in einer Anwendung beteiligt. Sie haben dann den Status „Externe“.

Sofern Nutzer*innen den Status eines Mitglieds erhalten, sind hieran besondere Bedingungen geknüpft. Derartige externe Nutzer*innen verfügen damit über ein Nutzerkonto der verantwortlichen Stelle. Nutzername, Rechtevergaben, ggf. eine alternative E-Mailadresse, Vor- und Nachname, ggf. die Organisation der externen Personen oder eine Telefonnummer, werden zusätzlich in MS-Azure sowie in den Berechtigungsmanagementsystemen der verantwortlichen Stelle erfasst. Über Anmeldungen und Veränderungen der Rechtevergaben werden automatisierte Logfiles für die letzten 30 Tage aufgezeichnet. Eine Auswertung solcher Logfiles erfolgt nur anlassbezogen zu legitimen Zwecken.

Externe Nutzer*innen mit dem Status „Gast“ sind die bevorzugte Wahl der Beteiligung der Zurverfügungstellung von Anwendungen durch die verantwortliche Stelle. Es werden dabei nur der Benutzername, in der Regel ist dieses die E-Mailadresse des Gast-Nutzers, Vor- und Nachname und ggf. die Organisation sowie Kontaktdaten verarbeitet. Es werden dabei nur Telemetriedaten und Logfiles im Rahmen der Aktivitäten in den berechtigten Anwendungen erfasst.

Aufgrund von Sicherheitseinstellungen kann im Einzelfall die Anmeldung bei einer Anwendung oder auf einem Gerät nur mit einer 2-Faktor-Authentisierung möglich sein. In diesem Zusammenhang können Mobilnummern verarbeitet werden und/oder es kann Kenntnis darüber erlangt werden, welch Art eines mobilen Endgeräts für die 2-Faktor-Authentisierung genutzt wird. Derartige personenbezogene Daten werden zu keinem anderen Zweck als der technischen Umsetzung der 2-Faktor Authentisierung verarbeitet. Sie werden mit Beendigung der Zurverfügungstellung eines Zugangs unwiederbringlich gelöscht.

Nutzer*innen mit dem Status „Externe“, welche lediglich über einen Link an verschiedenen Anwendungen teilnehmen, in der Regel nur durch Einsicht, werden anhand vergebener Namen, Vor- und Nachname, identifiziert. Zur Zusendung eines Links werden regelmäßig E-Mailadressen dieser Personen verarbeitet. Zur Teilnahme werden Telemetriedaten verarbeitet und es werden Logfiles, analog zu Gast-Nutzer*innen, erfasst.

Die verantwortliche Stelle hat im Rahmen technischer und organisatorischer Maßnahmen (TOMs) verschiedene Verfahren zur fortlaufenden Überprüfung von Zugängen aller Nutzer*innen getroffen, um Datenschutz und Sicherheit der Zusammenarbeit zu gewährleisten.

Grundsätzlich werden keine Gerätedaten von Nutzern mit dem Status „Gast“ (ausgenommen im Rahmen der 2-Faktor.Authentisierung wie oben) oder „Externe“ erhoben. Es wäre theoretisch möglich sich solche Daten aus Logfiles von Microsoft zu besorgen. Die verantwortliche Stelle macht hiervon grundsätzlich keinen Gebrauch.

Externe Nutzer*innen, welche den Status Mitglied haben, sind mit ihrem zugeteilten Benutzernamen unter Umständen auch an einem oder mehreren digitalen Endgeräten oder Anwendungen angemeldet, wobei die Daten des genutzten Gerätes erfasst werden. Grundsätzlich werden solche Informationen über Geräte, sofern es keine eigenen Geräte der verantwortlichen Stelle sind, nur zu folgenden Zwecken überwacht und ausgewertet:

- Überwachung einer angemessenen Sicherheit der Endgeräte, auf welchen sich ein „Mitglied“ angemeldet hat, um die Sicherheit von Daten und Anwendungen zu gewährleisten.
- Hilfe und technischer Support bei Problemen mit Anmeldungen, Anwendungen oder Endgeräten.
- Im Rahmen einer Bearbeitung von Daten in Anwendungen zur Erfassung von Logfiles für eine Rückverfolgbarkeit der Änderungen und Versionsverläufe.

Die vorgenannte Speicherung und Verarbeitung der Daten erfolgt auf der Grundlage eines berechtigten Interesses der verantwortlichen Stelle gem. Art. 6 Abs. 1 lit. f.) DS-GVO und insbesondere auch zur Umsetzung der aus Kapitel 4 DS-GVO bestehenden Pflicht geeignete Maßnahmen zu treffen, um Datenschutzverletzungen aufklären zu können. Hierbei wird diese Pflicht mit dem Grundsatz der Datensparsamkeit von der verantwortlichen Stelle sorgsam abgewogen.

Im Rahmen der Aufbewahrung von personen-bezogenen Daten zur potentiellen zukünftigen Aufklärung von möglichen Datenschutzverletzungen., erfolgt eine solche Aufbewahrung von Logfiles zugriffsbeschränkter Form. Die Dauer beträgt maximal 3 Jahre analog zu gesetzlichen Verjährungsfristen. Sie kann im Einzelfall deutlich geringer sein, wenn ein Zweck im vorgenannten Sinne nicht mehr vorliegt.

Sofern die verantwortliche Stelle einem Mitglied eigene Endgeräte aus deren Eigentum zur Verfügung stellt, gelten die hierfür getroffenen individuellen Absprachen und die auf dieser Grundlage verarbeiteten personenbezogenen Daten. Rechtsgrundlage ist sodann Art. 6 Abs. 1 lit. b.) DS-GVO.

Sofern ein Mitglied eigene private Endgeräte (BYOD) nutzt, gelten strenge Vorschriften zum Schutz der Privatsphäre des Mitglieds. Anmelde- und Geräteinformationen werden nur nach dem Minimalprinzip zum Zweck der technischen Zurverfügungstellung und Sicherheit gespeichert und verarbeitet. Private Geräte werden grundsätzlich nicht durch die verantwortliche Stelle verwaltet.

Durch Sicherheitsrichtlinien können Apps oder deren Funktionen, welche über eine Anmeldung eines Mitglieds oder eines Gasts betrieben werden, beschränkt werden. Dieses erfolgt grundsätzlich aus der jeweiligen App heraus ohne einen Eingriff in das private Endgerät dieser Personen.

Folgende M365 Anwendungen generieren grundsätzlich Telemetriedaten:

- Teams
- Exchange (E-Mail / Kalender)
- Sharepoint
- OneDrive
- Yammer
- Skype for Business
- Azure

Zusätzliche Telemetriedaten zu diesen Anwendungen, über die der der verantwortlichen Stelle in den Admin-

Centern zur Verfügung stehenden Telemetriedaten, könnten von Microsoft abgefordert werden. Die verantwortliche Stelle macht von solch einer Möglichkeit grundsätzlich keinen Gebrauch. Nur im Falle der Verfolgung von Straftaten oder zur Abwehr von Rechtsansprüchen würde eine Abfrage von Microsoft erfolgen, wenn diese zweckdienlich ist. Dieses erfolgt sodann auf der Grundlage eines berechtigten Interesses nach Art. 6 Abs. 1 lit. f.) DS-GVO.

Allgemeine Informationen zum Datenschutz bei Microsoft finden Sie unter folgendem Link: Übersicht über die Datenschutz- & Datenverwaltung - Microsoft Service Assurance | Microsoft Learn

Microsoft unterteilt in M365 Daten in folgende Klassifikationen:

- Kundeninhalte
- Identifizierbare Informationen über Endbenutzer (EUII)
- Pseudonymisierte Endbenutzer (EUPI)

Die Aufbewahrung von Kundeninhalten beträgt, bei aktiver Löschung durch den hierfür lizensierten M365 Benutzer maximal 30 Tage nach Löschung. Im Falle einer passiven Löschung von Kundeninhalten durch Microsoft erfolgt die Aufbewahrung nach Löschung maximal 180 Tage.

Unter die Kategorie EUII fallende personenbezogene Daten werden nach aktiver oder passiver Löschung für maximal 180 Tage bei Microsoft aufbewahrt. Administratoren der M365 Anwendung ist es möglich auf die Fristen der Aufbewahrung bei Microsoft für einer Widerherstellung Einfluss zu nehmen.

Unter die Kategorie EUPI fallende personenbezogene Daten werden maximal 30 Tage nach aktiver Löschung durch einen M365 Nutzer aufbewahrt. Im Falle der passiven Löschung beträgt die Frist maximal 180 Tage.

Im Falle der kompletten Kündigung eines M365 Abonnements werden die Kundendaten des Kontos in einer eingeschränkten Form bei Microsoft für 90 Tage vorgehalten und stehen dem dann ehemaligen Abonnementinhaber zur Einsicht zur Verfügung. Spätestens nach 180 Tagen werden solche Daten bei Microsoft final gelöscht.

Es besteht ferner die Möglichkeit der Beantragung der sofortigen Löschung von Daten durch hierfür berechtigte M365 Nutzer bei Microsoft. In einem solchen Fall werden die für die Löschung beantragten Daten final und unwiederbringlich binnen 72 Stunden gelöscht.

Zur Allgemeinen Sicherheit und zu technischen und organisatorischen Maßnahmen betreffend des Schutzes von Daten in der Microsoft Cloud, informiert Microsoft unter folgenden Link: Führungslinie zur Risikobewertung für Microsoft Cloud - Microsoft Service Assurance | Microsoft Learn

Es wird darauf hingewiesen, dass die Nutzung von M365 unabhängig einer Nutzung von Microsoft Windows oder anderer Microsoft Produkte außerhalb von M365, wie zum Beispiel den edge Explorer, für Endnutzer steht. Die in Verbindung mit M365 bestehenden Datenschutzrichtlinien betreffen diese Anwendungen nicht und geben auch keinen Hinweis darauf, wie Microsoft Datenschutz in anderen Anwendungen umsetzt.