Familienhilfe NORD
Helfende Hände in HH-Nord, Norderstedt und Umgebung

Datenschutzinformationen zur Speicherung und Verarbeitung von personenbezogenen Daten in Microsoft365

Wir nutzen in unserem Träger Dienste der Anwendung Microsoft 365 (M365, vormals Office365) mit welchen wir uns übermittelte Daten speichern und verarbeiten oder eine Zusammenarbeit im Träger als auch mit externen Personen betreiben. Betroffen von dieser Datenverarbeitung sind Mitarbeiter*innen, Geschäftspartner*innen und Klient*innen.

Verantwortliche Stelle für das Betreiben und die Bereitstellung von M365-Diensten ist:

Familienhilfe Nord Zübeyde Tas
Inhaberin: Zübeyde Tas
Europaallee 4, 22850 Norderstedt
Telefon: 040 / 60 92 75 95
E-Mail: info@familienhilfe-nord.de

Wir haben einen Datenschutzbeauftragten bestellt:

Tobias Lange
Externer Datenschutzbeauftragter
Berner Heerweg 246, 22159 Hamburg
Telefon: 040 5700 3925
E-Mail: info@tl-datenschutz.de

Es gelten im weiterem, sofern allgemeiner datenschutzrechtlicher Natur und in Hinblick auf die Ihnen zustehenden Rechte, unsere Datenschutzinformationen für Klient*innen und Geschäftspartner*innen bzw. Mitarbeiter*innen, welche Sie auf unserer Webseite finden können oder gerne jederzeit von uns übermittelt bekommen.

Wir haben 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 Bedingungen für die verschiedenen Dienste unter M365 zur Verfügung.

Grundsätzlich handelt es sich bei M365 um eine cloudbasierte Anwendung. Daten, auch personenbezogene Daten, werden zentral auf Servern von Microsoft und deren Subunternehmen gespeichert und verarbeitet.

Soweit wir Anwendungen für eine Zusammenarbeit als Auftragsverarbeiter im Sinne des Art. 28 DS-GVO dritten juristischen Personen oder deren Bediensteten zur Verfügung stellen, schließen wir mit Ihnen einen Auftragsverarbeitungsvertrag (AVV) ab.

Grundsätzliches zu Microsoft:

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. Das Abkommen soll in der ersten Hälfte des Jahres 2023 in den Status eines Angemessenheitsbeschlusses (Art. 45 DS-GVO) gehoben werden. 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 Zusammenhang sei erwähnt, dass die Ermittlung als auch Prävention von bzw. vor Straftaten elementarer Bestandteil der Ordnung eines jeden demokratischen Rechtstaates sind. In Deutschland ist dieses in der StPO §§ 100a ff. geregelt. Hiernach ist es den Staatsanwaltschaften, die in Deutschland nicht unabhängig sind, erlaubt, sogar über kurze Zeiträume ohne richterlichen Beschluss, Daten von Unternehmen der Privatwirtschaft zu erhalten und zu verarbeiten. Ferner diese Daten auch ohne eine Mitteilung an die betroffenen Personen zu verarbeiten, um Ermittlungsergebnisse 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 Datenerhebung und Verarbeitung in strafrechtlichen Ermittlungsverfahren

als in den USA, jedoch, in der Gesamtschau, ein vergleichbares Datenschutzniveau aus Sicht betroffener Personen

Unser Datenschutzbeauftragte überprüft regelmäßig die Entwicklung und die Informationslage zu staatlichen Datenschutzanfragen aus den USA unter vorgenannter Problematik und erstellt auf diesen Ergebnissen Einschätzungen zu einem vergleichbaren Datenschutzniveau zur DS-GVO. Auf dieser Grundlage bewerten wir den Einsatz vom M365 regelmäßig neu.

Verarbeitung von Daten in M365:

Folgende Kategorien an Daten werden in M365 verarbeitet:

- Namensdaten (Vorname und Nachname)
- E-Mail-Adresse oder Benutzername
- Telemetriedaten
- Inhaltliche Daten

Unter Telemetriedaten sind maximal die Speicherung und Verarbeitung von Daten über die Art, die Zeit, die Dauer, die genutzten Geräte, die Software, die IP-Adressen und die Teilnehmer einer Zusammenarbeit zu verstehen. Unter Inhaltlichen Daten sind alle Dokumente, Informationen und Mitteilungen jeder Art zu verstehen, welche in den Chat-Verläufen geführt, für die Zusammenarbeit hochgeladen oder sonstig zur Verfügung gestellt 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 hat sich vertraglich verpflichtet, Namens-, Benutzer- und Telemetriedaten nur für den Zweck der technischen Bereitstellung und eines Supports für die M365 Nutzung zu verarbeiten. Diese Verpflichtung kann durch die verantwortliche Stelle, aufgrund der Komplexität der Anwendung und der Größe von Microsoft, nicht detailliert überprüft werden. Es wird auf die Zertifizierung des MS-Rechenzentrums nach DIN ES ISO/IEC 27001 und weitere Zertifizierungen wie regelmäßige Prüfungen von Microsoft verwiesen. Ferner werden regelmäßig Marktbeobachtungen durch unseren Datenschutzbeauftragten durchgeführt, ob es Hinweise auf einen Abfluss von personenbezogenen Daten aus M365 gibt. Bisher konnten keine solchen belegbaren Szenarien festgestellt werden

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 gesonderten Aufbewahrungsfristen:

- 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 Kundenkorrespondenz darstellen (Empfang wie Versand), werden 6 Jahre aufbewahrt.
- E-Mails, soweit sie nicht unter Kundenkorrespondenz fallen, werden spätestens nach 12 Monaten automatisiert gelöscht, wenn ein Zweck nicht mehr fortbesteht.

Die vorgenannten Aufbewahrungsfristen, sofern nicht 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.

Abweichend zum Vorgesagten können einzelne Daten, auch personenbezogene Daten, in M365 als Kundenkorrespondenz, Sozialdokumentation oder aufgrund einer Relevanz für die Buchhaltung aufbewahrungs-pflichtig sein. Derartige Daten werden archiviert und entsprechend den gesetzlichen Bestimmungen in der Verarbeitung eingeschränkt vorbehalten. Rechtsgrundlage ist Art. 6 Abs. 1. lit. c.) DS-GVO. Im weiterem können Daten zu Zwecken der Abwehr oder Verfolgung von Rechtsansprüchen aufbewahrt werden. Rechtsgrundlage eines solchen berechtigten

Interesses ist Art 6. Abs. 1 lit. f.) DS-GVO. Im Falle eines strafrechtlichen relevanten Missbrauchs können Daten auf Rechtsgrundlage von Art. 6 Abs. lit. c.) verarbeitet werden.

Im Rahmen der Aufbewahrung von personenbezogenen Daten für eine zukünftige Aufklärung von möglichen Datenschutzverletzungen, erfolgt ggf. eine Aufbewahrung von Logfiles in zugriffsbeschränkter Form. Die Dauer beträgt maximal 3 Jahre analog zu den gesetzlichen Verjährungsfristen. Sie kann im Einzelfall deutlich geringer sein, wenn ein Zweck im vorgenannten Sinne nicht mehr vorliegt.

Aufgrund von Sicherheitseinstellungen kann im Einzelfall die Anmeldung an einem Endgerät, zu einer M365 Nutzung oder einer Zusammenarbeit nur mit einer 2-Faktor-Authentisierung möglich sein. In diesem Zusammenhang können Mobilnummern verarbeitet werden oder es kann Kenntnis über die Art eines mobilen Endgeräts für die 2-Faktor-Authentisierung erlangt werden. Derartige personenbezogene Daten werden zu keinem anderen Zweck als der technischen Umsetzung der 2-Faktor Authentisierung genutzt. Sie werden mit Beendigung der M365 Zusammenarbeit oder Nutzung unwiederbringlich gelöscht.

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

Mitarbeiter*innen der verantwortlichen Stelle haben grundsätzlich den Status Mitglied, externe Personen in der Zusammenarbeit den Status Gast oder externe Nutzer*innen. Unter bestimmten gesonderten Umständen können externe Personen einen Zugang mit einem Nutzerkonto unter der Domain der verantwortlichen Stelle erhalten und damit den Status Mitglied bekommen.

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.

Die direkte Anmeldung an Diensten und Anwendungen von M365 kann nur durch Personen mit dem Status Mitglied oder Gast erfolgen. Es werden hierbei personenbezogene Daten in Form von Logfiles erhoben. Sofern es sich um eine Anmeldung an durch die verantwortlichen Stellen überlassenen Endgeräten handelt, auch personenbezogene Daten in Form von Logfiles dieser Anmeldungen.

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.

Grundsätzlich generieren alle Dienste und Anwendungen der M365 Zusammenarbeit personenbezogene Daten in Form von Telemetriedaten, wenn diese mit einer Anmeldung, welcher Art auch immer, genutzt werden. Folgende M365 Anwendungen generieren erweiterte Daten im Rahmen einer Zusammenarbeit oder speichern erweiterte Telemetriedaten:

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

Zusätzliche Telemetriedaten zu diesen Anwendungen, über die hinaus, welche der

verantwortlichen Stelle in den Admin-Centern zur Verfügung stehenden, könnten von Microsoft angefordert 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 oder öffentlichen Interesses nach Art. 6 Abs. 1 lit. c.) oder f.) DS-GVO.

Allgemeine Informationen zum Datenschutz bei Microsoft und zu M365 finden Sie unter folgendem Link: Übersicht über die Datenschutz- & Datenverwaltung - Microsoft Service Assurance | Microsoft Learn

Microsoft unterteilt in M365 gespeicherte 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 eine Widerherstellung Einfluss zu nehmen und diese ggf. zu verkürzen.

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 Administratoren 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 geschieht. Die in Verbindung mit M365 bestehenden Datenschutzrichtlinien betreffen diese Anwendungen nicht und geben auch keinen Hinweis darauf, wie Microsoft Datenschutz in anderen Anwendungen umsetzt. Allerding können auch solche Anwendungen mit M365 interagieren und ggf. Daten, auch personenbezogene Daten, verarbeiten. Wenn Sie hierzu, unter Bezug auf eine konkrete Anwendung von Microsoft, Fragen haben, wenden Sie sich gerne jederzeit an unseren Datenschutzbeauftragten.

Externe Nutzer*innen:

Die Teilnahme an einer Zusammenarbeit mit Anwendungen von M365 für externe Nutzer*innen ist freiwillig. Externe Nutzer*innen treffen ihre Entscheidung über die Teilnahme eigenständig und nach deren eigenen Ermessen. Regelmäßig erfolgt die Teilnahme externer Nutzer*innen ohne eine ausdrückliche schriftliche Einwilligung. Die verantwortliche Stelle betrachtet hierbei die Teilnahme externer Nutzer*innen an der Zusammenarbeit in M365 als Einwilligung aufgrund eines schlüssigen Verhaltens zu den Datenschutzbedingungen, unter welchen diese Zusammenarbeit erfolgt. Rechtsgrundlage ist somit Art. 6 Abs. 1 lit. a.) DS-GVO. Dieses Datenschutzinformationsblatt informiert die externen Nutzer*innen über diese Bedingungen, mögliche Risiken und bestehende Datenschutzrechte in Bezug auf M365.

Gast- und Externe Nutzer*innen, wie auch Mitglieder, haben alle Datenschutzrechte, die Ihnen nach Kapitel 3 der DS-GVO zustehen. Insbesondere besteht das Recht jederzeit die Zustimmung zur MS-Teams Zusammenarbeit widerrufen zu dürfen, ein Recht auf Auskunft über die verarbeiteten personenbezogenen Daten und ein Recht auf Löschung von personenbezogenen Daten. Das Recht auf Löschung kann eingeschränkt sein, wenn anderweitige Rechte diesem entgegenstehen.

Externe Nutzer*innen mit dem Status „Gast“ sind die bevorzugte Wahl der externen Beteiligung an der M365 Zusammenarbeit mit der verantwortlichen Stelle. Es werden dabei nur Benutzername, in der Regel die E-Mailadresse des Gast-Nutzers, Vor- und Nachname und ggf. die Organisation verarbeitet.

Personen mit dem Status „externe Nutzer*innen“, welche lediglich über einen Link an Teilen der M365 Zusammenarbeit teilnehmen, 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, über den Aufruf der Links erfasst.

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

Gast-Nutzer*innen und Nutzer*innen mit dem Status Mitglied:

Grundsätzlich gilt für Nutzer*innen mit dem Status Mitglied oder Gast das vorgenannte für externe Nutzer*innen.

Darüber hinaus gelten für Nutzer*innen mit dem Status Mitglied besondere Bedingungen. Derartige Nutzer*innen verfügen damit über ein Nutzerkonto der verantwortlichen Stelle. Nutzername, Rechtevergaben, ggf. eine alternative E-Mailadresse, Vor- und Nachname, ggf. die Organisation oder eine Telefonnummer, werden zusätzlich in MS-Azure sowie in den Berechtigungsmanagementsystemen 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.

Nutzer*innen mit dem Status Gast werden mit ihren eigenen E-Mailadressen, analog zu Mitgliedern und im gleichen Umfang, im MS-Azure erfasst. Zusätzlich wird erfasst, ob diese mit einer eignen M365 Azure AD, einem Microsoft-Konto oder anderweitig registriert sind.

Nutzer*innen mit dem Status Mitglied und Gast werden in Rollen- und Berechtigungsverzeichnissen der verantwortlichen Stelle geführt. In diesen Verzeichnissen werden Rechte der Nutzer*innen, der Zeitraum dieser Rechte und der Status erfasst. Grundsätzlich erfolgt dieses nur für die Dauer, für die ein Zweck einer solchen Verarbeitung vorliegt. Zweck ist die Erfüllung technischer und organisatorischer Bestimmungen zur Sicherheit von Daten und IT sowie der Aufklärung von Vorfällen. Rechtsgrundlage ist ein berechtigtes Interesse gem. Art. 6 Abs 1 lit. f.) DS-GVO. So gespeicherte und verarbeitete Daten werden, mit Setzung des Status „inaktiv“, hiernach noch maximal 12 Monate aufbewahrt und sodann unwiederbringlich gelöscht.

MS-Teams Anwendung:

Technische Verbindungen in einer MS-Teams Zusammenarbeit oder einer Videokonferenz sind grundsätzlich verschlüsselt. Es bestehen umfangreiche Sicherheitsmaßnahmen gegen das Eindringen und Abhören durch dritte Personen. Nähere Informationen hierzu von Microsoft finden sie auf folgender Webseite:

https://learn.microsoft.com/de-de/microsoftteams/teams-security-guide

MS-Teams Administratoren können Berichte über die Zusammenarbeit abfragen und Telemetriedaten verarbeiten. Hiervon wird nur anlassbezogen Gebrauch gemacht. Die verantwortliche Stelle kann dabei maximal Informationen über die Art der genutzten Endgeräte, Nutzernamen, Nutzungsart, Zeiten und Teilnehmer*innen gewinnen. Diese Daten werden grundsätzlich nur zu legitimen Zwecken der Überwachung, Dokumentation oder Nachverfolgung von Zusammenarbeit, insbesondere für die Klärung technischer Fragen, genutzt. Derartige Aufzeichnungen können für maximal 180 Tage in die Vergangenheit abgefragt werden. Neben derartigen Berichten kann jeder MS-Teams Teilnehmer eigene Supportdateien erfassen. Die verantwortliche Stelle nutzt diese Funktion nur zu Zwecken technischer Problemklärungen mit dem MS-Support unter ausdrücklicher Einwilligung der jeweiligen Nutzer*innen. Derartige Supportdateien enthalten zusätzlich Informationen über Endnutzer-IP-Adressen, verwendete Geräte und Browser/Apps. Sie können nur durch und unter Mitwirken des jeweiligen Endnutzers generiert werden.

Die verantwortliche Stelle hat Voreinstellungen installiert, wonach Nutzer*innen auf bestimmte Rollen, die ihren jeweiligen Aufgaben entsprechen, beschränkt sind. Insbesondere wurden auch Beschränkungen gegen Mitschnitt oder Aufzeichnungen von Zusammenarbeit getätigt. In diesem Zusammenhang sei erwähnt, dass eine

absolute technische Sicherheit gegen Mitschnitt, Aufzeichnung oder automatisiertes Auslesen der Zusammenarbeit auf Endgeräten nicht möglich ist. Die Verantwortung eines datenschutzkonformen Umgangs in der Zusammenarbeit in MS-Teams obliegt insoweit den jeweiligen Nutzer*innen, die mit der Teilnahme eigenständig den deutschen Rechtsnormen, insbesondere dem Datenschutz, unterliegen. Hierzu sei ausdrücklich erwähnt, dass auch jede Form einer Verarbeitung von personenbezogenen Daten zu Mobbing oder Diskriminierung grundsätzlich rechtswidrig ist. Es wurde seitens der verantwortlichen Stelle ein Verfahren installiert, welches Datenschutz-verletzung in der MS-Teams Zusammenarbeit, im Verhältnis zur schwere des Vorfalls, durch Hinweis, Mahnung, Beschwerdeverfahren bis hin zu Ausschluss aus der Zusammenarbeit sanktioniert.

Die verantwortliche Stelle überprüft externe Nutzer*innen und lässt nur solche Personen zur MS-Teams Zusammenarbeit zu, die ihrer gewonnen Überzeugung nach hinreichend mit den bestehenden Datenschutzrechten vertraut sind. Ggf. werden mit Zulassung einer Person zu einer Teams-Zusammenarbeit Verpflichtungen auf den Datenschutz eingeholt, wenn dieses den Umständen nach erforderlich ist. Letzteres ist insbesondere dann der Fall, wenn besonders schutzwürdige Daten im Sinne des Art. 9 oder sonstige sensible Daten in großer Zahl gespeichert und verarbeitet werden.

Die Zusammenarbeit in MS-Teams kann insbesondere auch durch Audio- und Videobesprechungen erfolgen. Eine Teilnahme an einer Besprechung mit Video ist grundsätzlich freiwillig und obliegt der Entscheidung der jeweiligen externen Nutzer*innen. Ein Mitschnitt von Video-besprechungen erfolgt grundsätzlich nur durch hierfür besonders geschulte Administratoren unter ausdrücklicher Zustimmung aller Teilnehmer*innen der Besprechung. Aus Sicherheitsgründen wird allen Nutzer*innen von Videobesprechungen empfohlen Hintergründe zur Ausblendung des übrigen Raums zu verwenden. Ferner wird empfohlen während einer Besprechung alle übrigen, insbesondere privaten oder mit sensiblen Daten versehenen Anwendungen, zu schließen, um ein versehentliches Teilen auszuschließen.