LUDWIGSBURG

Zusammenarbeit mit externen Teilnehmenden in Microsoft Teams Teams

Diese Nutzungsvereinbarung wird im Zusammenhang mit einer Einladung zur Zusammenarbeit in Microsoft Teams mit externen Teilnehmern abgeschlossen. Nachfolgende Erklärung gilt für eine

- Teilnahme eines externen Partners an einem Teams Team (SharePoint) der Stadt

Zweck und Rechtsgrundlage der Verarbeitung

Die Verarbeitung personenbezogener Daten ist auf die Informationen zu beschränken, die für den jeweiligen Zweck notwendig sind (Artikel 5 Absatz. 1 lit. c Datenschutzgrundverordnung, kurz DSGVO. Die rechtliche Zulässigkeit bestimmt sich dabei maßgeblich an den Vorgaben des Artikel 1 Absatz 1 DSGVO. Eine Verarbeitung darf nur aufgrund einer Einwilligung der betroffenen Person oder weiteren von der DSGVO vorgegebenen Rechtsgrundlagen gemäß Artikel 6 DSGVO in Verbindung mit §§ 4 ff Landesdatenschutzgesetz, kurz LDSG von Baden-Württemberg erfolgen.

Für die Einbeziehung Dritter, in diesem Fall Microsoft als Anbieter der Clouddienste, gelten die weiteren Bestimmungen der Artikel 28 und 29 DSGVO sowie bei Datenübermittlungen an Drittländer Artikel 44 ff. DSGVO.

Die DSGVO und die nationalen Datenschutzgesetze verlangen, dass personenbezogene Daten zu löschen sind, wenn sie nicht mehr erforderlich sind. Dies wäre z.B. der Fall, wenn die Daten nicht zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind oder der Pflicht zur Datenlöschung keine gesetzlichen Aufbewahrungsfristen entgegenstehen. Die Einhaltung der datenschutzrechtlichen Vorgaben ist auch von den externen Teilnehmenden zu gewährleisten.

Teilnahme und Zugang: wer darf in MS Teams eingebunden werden?

Die Teilnahme an externen Teams und die Teilnahme von externen Personen an LB Teams zur Erfüllung und Wahrnehmung dienstlicher Aufgaben und Interessen sowohl in Teams Meetings als auch bei kollaborativer Zusammenarbeit in Teams (SharePoint) ist auf Stadtseite ausschließlich mit dem dienstlichen Account, bei externen Partnern mit geschäftlichen Adressen/Zugangsdaten (E-Mail etc.) zulässig. Der Zugang ist vor Zugriff von Unbefugten zu schützen.

Bis zum Abschluss der Zusammenarbeit ist der eingerichtete Zugang jederzeit zu gewährleisten, technische Störungen sind davon ausgenommen.

Der Abschluss der Zusammenarbeit muss den Teilnehmenden der Stadt /Externen in Stadt Teams in Absprache mit dem Besitzer des Teams rechtzeitig mitgeteilt werden. Weiter ist ausreichend Gelegenheit zu schaffen, eigene Daten aus der Zusammenarbeit herunterzuladen. Das Herunterladen von Projektdaten von weiteren Teilnehmenden darüber hinaus darf nur in Absprache mit dem/der jeweiligen Teams-Verantwortlichen zu erfolgen.

Übertragung von Bildschirm und Kamerabild: was ist zu beachten?

Der Einsatz der Kamera/Videofunktion ist freiwillig.

Vor der Nutzung der Kamerafunktion (Videokonferenz) sollte das Arbeitsumfeld (zum Beispiel. der von der Kamera erfasste Hintergrund oder Schreibtisch) auf vermeidbare Datenveröffentlichungen (zum Beispiel Whiteboards mit Projektskizzen) überprüft werden. Der Hintergrund sollte vorsorglich ausgeblendet werden.

Vor Nutzung der Funktion der Bildschirmübertragung (Desktop-Sharing) sollten Mail-Programme und Messenger-Programme (Vermeidung von Popup zu neuen Mails oder Nachrichten) geschlossen werden. Statt der kompletten Bildschirmfreigabe kann die Fenster-Freigabe genutzt werden, welche die Freigabe auf ein ausgewähltes Fenster beschränkt.

Die in Microsoft Teams integrierte Funktion der Präsenzanzeige dient dem alleinigen Zweck, die Kontaktaufnahme der Teilnehmenden untereinander zu verbessern, insbesondere bezüglich der Verwendung der dabei genutzten Medienkanäle (zum Beispiel. Video, Audio oder Chat). Beide Seiten sind sich einig, dass diese Ziele nur unter Wahrung der Persönlichkeitsrechte erfolgen und das System nicht zur Leistungs- oder Verhaltensüberwachung eingesetzt werden darf.

Aufzeichnung von Videokonferenzen

Die Aufzeichnung der Videokonferenzen ist nur erlaubt, wenn es vorher angekündigt wurde und der Speicherort zum Abrufen der aufgezeichneten Sessions allen Beteiligten bekannt und zugänglich ist. Ein unbefugtes Abhören oder Aufzeichnen während der Nutzung ist untersagt. Hierbei wird ausdrücklich auf die Strafbarkeit bei Verstoß nach § 201 Strafgesetzbuch, StGB hingewiesen.

Teilen von Daten

Wem gehören die Daten?

Beim Teilen von Dateien (Hochladen, Bildschirm teilen) bleibt das Eigentum an den Daten bei der liefernden Partei. Ein weiteres Teilen oder Verwenden der Daten über das Team hinaus ist ohne Genehmigung der liefernden Partei untersagt.

Wer bekommt Zugriff?

Auf die in einem Arbeitsraum eingestellten Dokumente können grundsätzlich alle Teilnehmer des Arbeitsraumes zugreifen, es sei denn, der Besitzer des Dokuments schränkt diese Berechtigung ein. Dateien die gemeinsam erarbeitet/bearbeitet werden, bedürfen ebenfalls für die Verwendung über das Team/den Teilnehmenden hinaus einer Information und Abstimmung mit Teilnehmenden und dem beziehungsweise der Teams-Verantwortlichen.

Bei Erweiterung des Arbeitskreises, Teams um zusätzliche Teilnehmende ist dies im Vorfeld mit den bereits vorhandenen Teilnehmenden zu klären und bei Bedarf ausreichend Zeit zu lassen datenschutzrelevante Themen zu behandeln und zu klären. In diesem Zusammenhang wird ausdrücklich ausgeschlossen, dass Daten aus Microsoft Teams an Big Data-Hintergrundsysteme weitergegeben werden dürfen.

Was darf geteilt werden?

Mitarbeiterbezogene Metadaten (zum Beispiel Systemanmeldung, Benutzerstatistiken etc.) dürfen nur für technische Zwecke, zur Steuerung, technischen Optimierung des Systems und zur Gewährleistung der Betriebssicherheit genutzt werden. Zugriffsberechtigt auf diese Funktionen sind nur Personen, die für diese Aufgaben zuständig sind. Zulässig sind Kontrollen, die zur Sicherstellung eines ordnungsgemäßen technischen Betriebes, wie etwa zum Virenschutz, Einbruchserkennung, Spam und Phishing Prävention, Malware-Schutz, Schutz vor Datenverlust verwendet werden.

Bei der Nutzung der Kollaborationsplattform sind die geltenden rechtlichen Bestimmungen des Urheberrechtes zu beachten. Fremde Inhalte, deren Nutzung nicht durch freie Lizenzen zulässig ist, dürfen nur als Zitate verwendet werden. Die Quelle ist in jedem Falle anzugeben.

Widerrufsrecht bei Einwilligung

Wenn Sie in die Verarbeitung durch eine entsprechende Erklärung eingewilligt haben, können Sie die Einwilligung jederzeit für die Zukunft widerrufen. Die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird durch diesen nicht berührt.

Ich habe die vorstehenden Anweisungen gelesen und erkläre mich damit einverstanden

Ich erkläre außerdem, dass ich die datenschutzrechtlichen Bestimmungen und die Anforderungen an die IT-Sicherheit beachten werde. Diese habe ich als Anlage zu dieser Vereinbarung erhalten.

Anlage

Benutzer- und Rechteverwaltung

Teilnehmende dürfen nur so lange Mitglied des Teamsteams sein, wie es die Zusammenarbeit erfordert. Ist die Zusammenarbeit beendet oder scheiden Mitglieder aus, muss ihnen der Zugriff entzogen werden. Der Teamsbesitzer muss sicherstellen, dass er über das Ausscheiden von Mitgliedern umgehend informiert wird. Er ist außerdem dafür verantwortlich, den ausgeschiedenen Mitgliedern die Zugriffsrechte zu entziehen.

Diese Kontrollhandlungen sind wichtig, damit unautorisierte Zugriffe (z.B. nach Beendigung des Arbeitsverhältnisses) keinen weiteren Zugriff auf Microsoft Teams und die dort gespeicherten Daten haben. Soweit diese Vereinbarung mit externen Dienstleistern abgeschlossen wird, werden deren Mitarbeitende auf die Einhaltung dieser Bestimmungen verpflichtet.

Datensicherheit

Der Zugang von Externen an Teams der Stadt Ludwigsburg darf ausschließlich über geschäftliche beziehungsweise dienstliche Endgeräte/Devices erfolgen.

Diese sind speziell gehärtet und entsprechenden sicherheitstechnischen Anforderungen des BSI (vgl. IT-Grundschutz). Hierzu zählen zum Beispiel. das Einspielen aktueller Software-Patches und Antivirus-Signaturen sowie der Einsatz einer Firewall. Darüber hinaus sollten alle Zugangsrechte und Zugriffsrechte auf die Daten auf das notwendige Mindestmaß beschränkt sein. Dies ist bei privaten Endgeräten/Devices häufig nicht möglich, weshalb deren Nutzung verboten ist.

Die beteiligten Parteien haben dafür zu sorgen, dass sämtliche Maßnahmen zum Schutz der Daten ergriffen werden und nur Endgeräte/Devices zum Einsatz kommen, bei denen ein angemessenes Sicherheitsniveau umgesetzt ist. Die datenschutzrechtlichen Vorschriften der DSGVO und der nationalen Datenschutzgesetze sowie die gesetzlichen und verwaltungsinternen Regelungen für die Datensicherheit gelten auch beim Arbeiten mit Microsoft Teams und müssen uneingeschränkt gewährleistet werden. Auf die Einhaltung der spezifischen Anforderungen ist daher besonders zu achten. Entsprechendes gilt für den Zugang städtischer Mitarbeitenden in Teams von Externen.

Alle Daten, Informationen und Passwörter sind so zu schützen, dass Dritte weder Einsicht noch Zugriff darauf nehmen können. Passwörter müssen sicher sein und dürfen nicht erratbar sein. Sie müssen aus mindestens 8 Zeichen bestehen, worunter sich eine Zahl, ein Großbuchstabe und ein Sonderzeichen befinden müssen. Sollten die eigenen Zugangsdaten durch ein Versehen anderen Personen bekannt geworden sein, ist der Benutzer verpflichtet, sofort Maßnahmen zum Schutz der eigenen Zugänge zu ergreifen. Falls noch möglich, sind Zugangspasswörter zu ändern. Ist dieses nicht möglich, ist der Teams-Verantwortliche umgehend zu informieren.

Darüber hinaus müssen die Teilnehmer dafür Sorge tragen, dass Unbefugte (zum Beispiel im Haushalt lebende Personen etc.) keinen Zugang zur Kollaborationsplattform und den dort gespeicherten Daten erhalten. Mit der gleichen Sorgfalt ist sicherstellen, dass auch Zugriffe Unbefugter auf die IT-Systeme oder andere Datenträger ausgeschlossen sind. Dies beinhaltet insbesondere auch die datenschutzkonforme Entsorgung von Datenträgern. Unterlassen Sie es, wissentlich Beschränkungen des Zugriffs auf die Dienste oder deren Verfügbarkeit zu umgehen.

Die Nutzung von Microsoft Teams einschließlich der freigegebenen Dienste ist ausschließlich für dienstliche Zwecke und nur im ausdrücklich erlaubten Umfang zur Erledigung der übertragenen Aufgaben gestattet. Eine Kopplung mit privaten Konten oder anderen Diensten ist untersagt. Der Arbeitsplatz ist so zu organisieren, dass private und dienstliche Daten immer voneinander getrennt sind. Das heißt. Arbeitsmittel, Endgeräte/Devices oder überlassenen Systemzugänge dürfen nicht für private Zwecke genutzt werden und auch die Überlassung an Dritte ist untersagt.

Bei der Wahl eines geeigneten Arbeitsortes sind von den Teilnehmenden die für die Aufgabenerledigung erforderlichen Sorgfaltspflichten hinsichtlich der Vertraulichkeit der bearbeiteten Vorgänge zu berücksichtigen. Gerade bei der Arbeit in öffentlichen Umgebungen (zum Beispiel in der Bahn) besteht die Gefahr des „über die Schulter schauen" (Shoulder Surfing). Auch videoüberwachte Bereiche können ein Sicherheitsproblem darstellen, da hochauflösende Kameras alle Eingaben und den Inhalt des

Bildschirms aufzeichnen können. Daher muss grundsätzlich abgewogen werden, welche Tätigkeiten an öffentlichen Orten durchgeführt werden können und welche nicht.

Alle bestehenden Regelungen zum Datenschutz, zur Datensicherheit und hinsichtlich der technischen Möglichkeiten zur digitalen Zusammenarbeit und Kommunikation sowie deren Durchführung bzw. Umsetzung innerhalb der Kollaborationsplattform sind von allen Teilnehmenden zu beachten.

Datenschutz

Für die Zusammenarbeit soll Microsoft Teams genutzt werden. Die Kollaborationsplattform ist ein Service der Microsoft Corporation mit Sitz in den USA. Da das US-Gesetz „Cloud Act", welches den US-Geheimdiensten umfassende Rechte beim Zugriff auf die Daten einräumt, auch für europäische Tochterunternehmen Anwendung findet, kommt der Einhaltung der datenschutzrechtlichen Anforderungen innerhalb der Kollaborationsplattform eine besonders hohe Bedeutung zu. Das frühere EU-US Privacy Shield-Abkommen wurde mit EuGH-Urteil vom 16.07.2020 für ungültig erklärt.

Aus diesem Grund dürfen in Microsoft Teams derzeit keine personenbezogenen Daten abgelegt werden, die besonders schützenswert sind oder der Geheimhaltung unterliegen. Darüber hinaus dürfen auch keine Inhalte kommuniziert werden, die einem Dienstgeheimnis unterliegen. Ausgenommen hiervon sind ausschließlich folgende Datentypen:

- Angaben zum Benutzer (Name, Vorname, dienstliche Mailadresse, etc.)
- Meeting-Metadaten (Thema Beschreibung, Teilnahmedauer)
- Text-, Audio- und Videodaten, die durch die Anwender selbst veröffentlicht werden
- Standortinformationen

Die Profildaten sind erforderlich, um eine Identifikation der Teams-Mitglieder zu ermöglichen. Die Ergänzung um ein persönliches Bild und private Telefonnummern ist freiwillig. Weitere persönliche Daten werden nicht im System geführt.

Die jeweils gültigen Richtlinien für den Datenschutz und die Datensicherheit der Stadtverwaltung sind unbedingt zu beachten. Externe Teilnehmer sollten sich bei der Bewertung der jeweiligen Datentypen am **Schutzbedarf „normal"** (vgl.) oder dem **Vertrauensniveau „Substantiell"** (vgl. Kapitel 1.3 der Technischen Richtlinie TR-03107-1 „Elektronische Identitäten und Vertrauensdienste im E-Government") orientieren. Die Teilnehmenden sind für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich und müssen die in diesem Zusammenhang ergriffenen technischen und organisatorischen Maßnahmen entsprechend umsetzen.

Weitere Informationen zur Datenverarbeitung durch Microsoft entnehmen Sie bitte der Datenschutzerklärung des Herstellers (https://privacy.microsoft.com/de-de/privacystatement).

Übermittlung von personenbezogenen Daten in ein Drittland

Die Datenverarbeitung durch Microsoft 365 erfolgt vertragsgemäß auf Servern, die von Microsoft in einem europäischen RZ-Standort betrieben werden. Bei Microsoft Teams kann die Verarbeitung der Daten in einem EU-Mitgliedstaat, insbesondere bei erhöhter Systemauslastung, nicht garantiert werden. Dies führt in der Folge dazu, dass eine datenschutzkonforme Nutzung der Services ggfs. nicht gewährleistet werden kann. Deshalb ist die Verarbeitung personenbezogener Daten mit einem erhöhten Schutzbedarf mittels Microsoft Teams verboten.

Informationspflichten gemäß Art. 13 und 14 DSGVO

1. Name und Kontaktdaten Ihrer Kontaktperson

Stadt Ludwigsburg

Wilhelmstraße 11, 71638 Ludwigsburg

Fachbereich: Gesellschaftliche Teilhabe, Soziales und Sport - Pflegestützpunkt

Vorname und Name: Katrin Heilemann

Telefon: 07141 910 - 3123

Telefax: 07141 910 - 2464

E-Mail: rathaus@ludwigsburg.de

2. Kontaktdaten der behördlichen Fachperson für Datenschutz Wolfgang Müller

Telefon: 07141 910-2721

E-Mail: datenschutz@ludwigsburg.de

Betroffenenrechte

Nach der DSGVO stehen Ihnen folgende Rechte zu:

Werden Ihre personenbezogenen Daten verarbeitet, so haben Sie das Recht, Auskunft über die zu Ihrer Person gespeicherten Daten zu erhalten (Artikel 15 DSGVO).

Sollten unrichtige personenbezogene Daten verarbeitet werden, steht Ihnen ein Recht auf Berichtigung zu (Artikel 16 DSGVO).

Liegen die gesetzlichen Voraussetzungen vor, so können Sie die Löschung oder Einschränkung der Verarbeitung verlangen sowie Widerspruch gegen die Verarbeitung einlegen (Artikel 17, 18 und 21 DSGVO). Gegen die Datenverarbeitung aufgrund des Vertrags besteht kein Widerspruchsrecht.

Wenn Sie in die Datenverarbeitung eingewilligt haben oder einen Vertrag zur Datenverarbeitung besteht und diese mithilfe automatisierter Verfahren durchgeführt wird, steht Ihnen ggfs. ein Recht auf Datenübertragbarkeit zu (Artikel 20 DSGVO).

Sollten Sie von den oben genannten Rechten Gebrauch machen, prüft die Stadt Ludwigsburg, ob die gesetzlichen Voraussetzungen hierfür erfüllt sind.

Bei datenschutzrechtlichen Beschwerden können Sie sich an die zuständige Aufsichtsbehörde wenden:

Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg
Postfach 10 29 32
70025 Stuttgart
Telefon: 0711 615541-0
FAX: 0711 615541-15
E-Mail: poststelle@lfdi.bwl.de