Privacy Policy for "Microsoft Teams" of the Utimaco Group

In order to ensure consistency and alignment with our data protection practices, this privacy notice extends to all companies within our group, regardless of whether they are legally required to comply with the General Data Protection Regulation (GDPR) or other similar data protection regulations.

Please note that in cases where specific legal requirements or regulations are applicable to a particular group company, such additional or separate privacy requirements will apply, however, in a way to allow complementation and adherence to the overarching principles and standards outlined in this specific privacy policy for Microsoft Teams.

This ensures that our employees and stakeholders can have confidence in the way we handle personal information and respect individuals' privacy rights, regardless of their location.

1. Controller

The "Controller" within the meaning of the General Data Protection Regulation (hereinafter referred to as "GDPR") and other data protection regulations are

Utimaco Management Services GmbH
Germanusstraße 4
52080 Aachen
Germany

Utimaco GmbH
Germanusstraße 4
52080 Aachen
Germany

Utimaco Management GmbH
Germanusstraße 4
52080 Aachen
Germany

Utimaco IS GmbH
Germanusstraße 4
52080 Aachen
Germany

Utimaco TS GmbH
Germanusstraße 4
52080 Aachen
Germany

Utimaco TS UK Limited
9th Floor 107
Cheapside
London, EC2V 6DN
UK

Utimaco TS SRL
Milanofiori, Strada 6,
Edificio A, Scala 13,
20057 Milano, Italy

MYHSM Ltd.
Midshires House,
Midshires Business Park,
Smeaton Close
Aylesbury,
HP19 8HL
UK

conpal GmbH
Dornhofstraße 67-69,
63263 Neu-Isenburg
Germany

Realia Technologies, S.L.
Calle Infanta Mercedes,
número 90, 4º 28020 Madrid
Spain

- hereinafter collectively referred to as "Utimaco Group of Companies" or "we" –

In the following, we would like to inform you about the processing of personal data in connection with the use of the communication tool "Microsoft Teams" ("MS Teams") as well as the Microsoft Teams Teams functionality. MS Teams is part of the Microsoft Office 365 Cloud application. Microsoft Office is a software provided by Microsoft Ireland Ltd., One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland a subsidiary of Microsoft Corporation One Microsoft Way, Redmond, WA 98052-6399, USA (hereinafter: "Provider").

You can use MS Teams if you enter the respective meeting ID and, if applicable, other access data for the meeting directly into the provider's MS Teams app.

If you do not want to or cannot use the Microsoft Teams app, then the basic functions can also be used via a browser version, which you can also find on the provider's website.

2. Purpose of processing

We use MS Teams to conduct chats, conference calls, online meetings, video conferences and/or webinars (collectively, "Online Meetings") ("Processing Activity").

Personal data is processed to facilitate collaboration and communication between our employees and with external parties. Personal data is used to ensure that our employees can use the services offered by Microsoft Teams and related Microsoft products and interact with others through Microsoft Teams meetings, chat messages, channel messages, audio and video calls, file sharing, collaborative document creation, and so on. We process your personal data for the purpose of organizing virtual meetings and conversational chats. The personal data is collected and stored on Microsoft's cloud servers. Purpose is providing the above services.

The Teams Teams function is administered in a standardized way through the EasyLife tool (EasyLife 365) tool as further set forth herein. Sharing of files is permitted in these groups internally and with external parties as set further herein and you can establish Teams groups via this tool.

MS Teams is not used for the purpose of automated decision-making within the meaning of Article 22 GDPR.

3. What data is processed?

3.1 Microsoft Teams

When using MS Teams, different types of data are processed depending on the content, purpose, occasion and scope of use. The scope of the data depends on what information you provide before or when participating in an online meeting. The following personal data categories are subject to processing:

User information: The amount of user information collected depends on whether you are an employee of Utimaco or an external user.

The following data is displayed by employees: ad name ("display name"), first name, last name, telephone (optional), internal company e-mail address, office space (optional) profile picture (optional), department/employer and position (optional), preferred language.

The data of external users are visible as follows: ad name, first and last name (optional), telephone (optional), e-mail address, and profile picture (optional).

Screen sharing: Participants have the option of screen sharing. When this feature is enabled, the entire content of the shared screen or program window is displayed to the other participants.

Metadata: subject, description (optional), attendee IP addresses, device/hardware information, meeting ID, date, time, location, and phone numbers as well as access and process data, including interaction data, diagnostic data, user activity, communication content and shared files. However, this is only possible for administrators. Utimaco may also control and manage employee responsibilities, including control of privacy-related settings.

Recordings: (M4A file of all audio recordings, and a text file of online meeting chat): The recording function is switched off by default but can be switched on individually by the users. This cannot be influenced by us. Before recording, a corresponding notification appears to each participant.
The fact of recording is also displayed in the upper left corner of the application as "Recording" in the MS Teams app. If you want to record online meetings, please inform others transparently in advance and – if necessary – ask for consent.

Dialing in by telephone: Information on incoming and outgoing phone numbers, country name, start and end time. If necessary, further connection data such as the IP address of the device may be stored.

Text, audio, and video: You may have the option to use chat, question, or survey features in an online meeting. In this respect, the text entries made by you will be processed to display them in the online meeting and, if necessary, to log them. To enable the display of video and the playback of audio, the data from the microphone of your terminal device and any video camera of the terminal device will be processed accordingly during the duration of the meeting. You can turn off or mute the camera or microphone yourself at any time using the corresponding Microsoft Teams applications.

Chat messages can be viewed by all participants. The chat content is also logged by Microsoft Teams when used. The respective participants can download the chat logs before leaving the online meeting. Logging chats should only be performed where there is a business need. Files that users share in chat are stored in the OneDrive for Business account of the user who shared the file.

Attention tracking: The possibility of software-based "attention tracking" in online meetings is disabled.

3.2 Additional data processing relating to Microsoft Teams Teams functionality/EasyLife 365

When using MS Teams Teams functionality, different types of data are processed depending on the content, purpose, occasion and scope of use. The scope of the data depends on what information you provide when contributing to the collaboration groups within Teams Teams or when participating in an online meeting.

Apart from the abovementioned data, the Teams Teams (Easylife 365) functionality also processes data related to Customer history, audit logs, payment data, data related to the use of the product, activity logs for troubleshooting purposes and data related to your Microsoft environment such as domain information etc.

3.3 Avoid sharing sensitive data

Please note that neither we nor the provider can control what you share in meetings and conversational chats. We strongly discourage you from using Microsoft Teams to share sensitive data - data revealing a natural person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data (mental and physical), and data about a natural person's sex life or sexual orientation - about yourself or other natural persons.

4. Legal basis of data processing

For employees of the Utimaco Group, § 26 of the Federal Data Protection Act (hereinafter: "BDSG") is the legal basis for data processing. According to § 26 BDSG, the processing of personal data may take place for the execution of the employment relationship. If necessary, we process your data beyond the actual fulfilment of the employment relationship to safeguard our legitimate interests or those of third parties, provided that your interests or fundamental rights and freedoms that require the protection of personal data do not prevail (Article 6 para. 1 f) GDPR). In these cases, we are interested in the effective conduct of online meetings. Further details can be found in the data protection information for employees of the Utimaco group of companies.

For other participants in online meetings – insofar as the meetings are carried out within the framework of contractual relationships – Article 6 para. 1 lit. b) GDPR is the legal basis for data processing. If there is no contractual relationship, the legal basis is Article 6 para. 1 lit. f) GDPR. Here, too, we are interested in the effective conduct of online meetings.

For the purposes of MS Teams functionality, we process your data to safeguard our legitimate interests or those of third parties, provided that your interests or fundamental rights and freedoms that require the protection of personal data do not prevail (Article 6 para. 1 f) GDPR).

5. Recipients / Disclosure of personal data

The personal data will be disclosed to the following recipients on the need to know basis:

- employees and external users, who are part of the online meetings;
- Utimaco to the extent necessary to provide the Service;
- Microsoft and Microsoft's sub-processors to the extent necessary and involved in the data processing.

The access to personal data through Microsoft and Microsoft's sub-processors is limited through the implementation of a so called bring-you own-key solution by Utimaco. This includes that a key is generated regularly by a Utimaco HSM and stored in the MS Secure Store which encrypts all data in Utimaco's Microsoft Tennant. Microsoft has no access to the key and therefore no access to unencrypted data. Only in very limited support cases Utimaco would grant dedicated persons in Microsoft a temporary authorization via a secure process to unencrypted data (e.g. log files) for the purpose of problem solving only.

Other third parties will not have access to your personal data unless required by law.

6. Data processing outside the European Union

Utimaco took advantage of the option offered by Microsoft Teams to set the location. For all data processed in Germany, the storage location is Germany, for data processed in Italy, the storage location is Italy and at all other locations (e.g. United Kingdom, USA) also determines the storage location Germany.

Since Microsoft is a service provided by a provider based in the United States, a data transfer to the U.S: cannot be excluded and can result in risks for users, as it can be more difficult, for example, to enforce the rights of data subjects.

We have concluded a data processing contract with the Microsoft, which meets the requirements of Article 28 GDPR and guarantees an adequate level of data protection through the conclusion of the so-called EU standard data protection clauses published by the EU Commission on June 4, 2021 pursuant to Article 46 para. 2 c) GDPR and contains other suitable guarantees concerning enforceable rights and remedies of data subjects.

In addition, according to Article 45 GDPR, personal data may be transferred to a third country (e.g., the USA) if the EU Commission has decided that the third country in question offers a level of data protection that complies with the GDPR. The European Commission signed the adequacy decision for the new data protection framework agreement between the United States and the European Union (EU) on July 10, 2023. This means the agreement, also known as the Data Privacy Framework, has entered into force. The Commission has thereby confirmed that the United States provide an adequate level of protection for personal data comparable to that provided by the EU. The prerequisite is that the US company in question is certified accordingly with the US Department of Commerce which is the case. Microsoft's certification status can be viewed at: https://www.dataprivacyframework.gov/s/participant-search/participant-detail

Against this background, the transatlantic data transfer between us and our US service provider can be legally performed.

The provider also reserves the right to process customer data for its business purposes. Please note that we have no influence on the data processing by the provider. To the extent that Provider processes Personal Data in connection with legitimate business operations, the Provider is an independent data controller for such use and, as such, is responsible for complying with all applicable laws and obligations of a data controller.

Further information on the purpose and scope of data collection and processing by the provider can be found in the data protection declaration under https://learn.microsoft.com/de-de/microsoftteams/teams-privacy and https://docs.microsoft.com/de-de/microsoftteams/teams-privacy. There you will also find further information on your data subjects rights in this regard.

Furthermore, processing takes place outside the EU if participants in online meetings attend from a third country. However, the data is encrypted during transport over the internet and thus protected against unauthorized access by third parties.

7. Technical and organizational security measures

The Utimaco group of companies has established technical and organizational security measures for the use of MS Teams, which, where applicable, should also be followed by you. These include in particular:

- Two-factor authentication for employees;
- Information encryption to protect personal data;

- Use of the option of the so-called "waiting room", which allows the identity of the external user wishing to participate to be verified in the context of an online meeting/conference before being approved by the initiator of the conference;
- Rapid installation of provided updates;
- No unauthorized disclosure of the transmitted Online Meeting ID;
- No posting of pictures of the online meeting;
- No public provision of the meeting link;
- Internal telecommunications should only exceptionally take place via MS Teams; Employees should use the IP telephony application provided by Utimaco by default;
- Manual setting options for the benefit of users regarding their availability via MS Teams, read receipts in chat histories, background recordings in video conferences;
- Additional apps in MS Teams are administratively deactivated and only activated for use;
- File shares are blocked through the internal firewall;
- Determine what kind of information can be exchanged in the meeting. You should not disclose any personal information about yourself or anyone else in the Application, except as strictly necessary. For example, the user's accessibility information can be set as "appear offline" and read receipts in chats can be switched off;
- If possible, particularly sensitive data should not be exchanged in video conferences.
- By disabling the AutoStart for MS Teams, you can prevent the program from starting automatically when your device boots;
- Recording, photographing or similar functions in meetings are prohibited without the consent of the participants. It is better to send such data separately before or after the meeting. In particular, meetings should only be recorded in exceptional cases and only to the extent necessary;
- The recording function should always be stopped when the person who started the recording leaves the online meeting.
- Participants should always end the online meeting when they leave it.
- Information about other participants, other persons, trade secrets or other sensitive information disclosed during the meeting shall be treated confidentially;
- For meeting invitations, send the password separately from the meeting ID if possible.

8. Data Protection Officer and Data Protection Coordinator

We have appointed a data protection officer and a data protection coordination team.
You can contact our data protection coordination team as follows:

Utimaco Management Services GmbH
– Data Protection Coordination Team–
Germanusstrasse 4
52080 Aachen, Germany
Germany
E-mail: dataprotection@utimaco.com

9. Your rights as a data subject

Upon request, you have the right to receive information free of charge as to whether and which data about you is stored and for what purpose the storage takes place (Article 15 GDPR). In the case of a request for information that is not made in writing, we ask for your understanding that we may require proof from you that you are the person you claim to be. The restrictions of § 34 BDSG apply.

You have a right to rectification or erasure or restriction of processing, insofar as you are legally entitled to do so.

In accordance with Article 21 GDPR, you have the right to object to the processing of personal data concerning you. Further information can be found in the section "Information about your right to object according to Article 21 GDPR below.

A right to data portability also exists within the framework of the data protection requirements according to Article 20 GDPR. Thereafter, you have the right to receive your data from us in a structured, common and machine-readable format. Forwarding to another responsible person may not be hindered by us.

10. Deletion of data

We delete personal data if there is no need for further storage. A requirement may exist in particular if the data is still required to fulfil contractual services, to check the warranty and, if applicable, to grant or defend warranty claims. In the case of statutory retention obligations, deletion is only considered after the expiry of the respective retention obligation. Corresponding proof and retention obligations arise, among other things, from the German Commercial Code and the Tax Code. The storage periods are then up to ten years. If required, we will be happy to provide you with further information on the duration of data storage concerning the specific purpose.

Pursuant to the MS Teams Team functionality through the Easy Life tool, the team groups are automatically archived after 30 days of inactivity and accesses are no longer possible from outside or inside.

11. Right to complain to a supervisory authority

You have the right to complain about our processing of personal data to a competent supervisory authority for data protection.

12. Information about your right to object according to Article 21 GDPR

Right to object on a case-by-case basis

You have the right, for reasons arising from your particular situation to object at any time to the processing of personal data concerning you, which is based on Article 6 para.1 f) GDPR.

If you object, we will no longer process your data unless we can demonstrate compelling legitimate grounds for the processing which outweigh your interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims.

The objection can be made informally with the subject "objection" stating your name, address and date of birth and should be addressed to the data protection coordinator of the Utimaco Group, whose contact details you will find in section 8 of this notice.

13. Changes to this Privacy Policy

We revise this data protection information in the event of changes in data processing or other occasions that make this necessary. The current version can always be found on our website or is available on request.

14. Automated individual decision-making, including profiling

Within the scope of the use of MS Teams, there is no fully automated decision-making (including profiling) according to Article 22 GDPR. Should we use these procedures in individual cases, we will inform you about this separately if this is required by law.

15. Learn more about Microsoft's privacy

https://privacy.microsoft.com/de-de/privacystatement
https://www.microsoft.com/de-de/trust-center