

Privacy Protection Information

Data Protection Information Provided in Accordance With Articles 13 and 14 of the EU General Data Protection Regulation (GDPR) Concerning Microsoft-Teams (Microsoft Teams)

Data Protection Information Concerning Online Meetings, Telephone Conferences and Webinars Held via Microsoft Teams

We will inform you hereafter about the processing of personal data related to use of the communication and collaboration platform, Microsoft Teams.

Controller

The controller for data processing related directly to “online meetings” is TÜV NORD Service GmbH & Co. KG: email: privacy@tuev-nord.de

Please note: When you access the Microsoft Teams website, the data processing controller will be the provider of Microsoft Teams. The Microsoft Teams application is a service of the Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399 USA.

However, to use Microsoft Teams, accessing the website is only necessary for downloading the “Microsoft Teams” software. For Microsoft Teams’ privacy statement, please see:

[Teams free support and privacy statement.](#)

Our Data Protection Officer

As a party to an agreement with the Microsoft Corporation, TÜV NORD Service GmbH & Co. KG appointed a Group data protection officer. You may also contact our data protection officer if you have any questions or suggestions concerning data protection (e.g., about access or updates to your personal data).

Berthold Weghaus
TÜV NORD AG
Email: privacy@tuev-nord.de

General Usage Information:

You may also use Microsoft Teams if you receive a Meeting ID and, if necessary, other access data by email or participate via the Microsoft Teams app.

If you do not want to or cannot use the Microsoft Teams app, its basic functions can also be used on a browser version provided on the Microsoft Teams website:

<https://www.microsoft.com/en-us/microsoft-teams/group-chat-software?rtc=1>

You may also participate in online meetings as a guest.

Please note that Microsoft Teams meetings cannot be held fully on unsupported browsers and may be subject to limitations, e.g., when approving cameras, monitors, content or microphones.

For further information about supported browsers, please see:

<https://docs.microsoft.com/en-us/microsoftteams/unsupported-browsers>

1 Processing

Data Processing Purposes

We use Microsoft Teams to hold telephone conferences, online meetings, video conferences and/or webinars.

The legitimate interest of our Group consists of simplifying internal communication, processing inquiries, improving efficiency and promoting cooperation across the Group and its branches.

Data Types and Data Subject Categories

Various types of data are processed when using Microsoft Teams. The scope of this data depends on which information you disclose before or while participating in an online meeting.

When actively using such offers, data of participants in communication will, if necessary for the communication, be processed and stored on servers of the third-party providers used.

Relevant personal data categories/types may especially include:

- Data subject categories:
- (Internal/external) participants in an online offer (conference, meeting, webinar)
- User information:
- Display name, email address, profile picture (optional), preferred language
- Data types:
- Master data (e.g., name, address), if applicable, pseudonyms, contact details (e.g., email address, telephone number), content data (e.g., entered text, images, videos), metadata and communication data (e.g., device information, IP addresses)

- Usage data and metadata:
- Time, date, Meeting ID, telephone numbers, location
- Text, audio and video data based on your consent:

Chat, question and survey functions may be used at online meetings. Text you entered will be processed thereby to be displayed at the online meeting and, if applicable, protocoled. To display videos and use audio, data from your device's microphone and camera will be processed during the duration of the meeting.

You may turn off or mute your camera or microphone at any time via the Microsoft Teams application.

If you participate in a video conference, you may also use background effects to conceal, e.g., your private surroundings. You may configure this individually during video conferences.

Which data Microsoft Teams collects and processes for which purpose is explained here:

<https://docs.microsoft.com/en-us/microsoftteams/teams-privacy>

Data Processing Scope

We will protocol chat content if necessary for protocoling results of online meetings. However, this will not normally be necessary.

Questions asked by webinar participants may also be processed for documentation and follow-up purposes.

Screen content may also be shared. In this case, we will know which data and content you share through your screen.

Recording Meetings

We will inform you transparently and in advance and request your consent if we would like to record meetings.

That a meeting is being recorded will be also displayed on the Teams app or browser view. Participants will receive notification which includes a link to privacy protection information for online participants.

The organizer may also choose which participants may record meetings.

We will protocol chat content if necessary for protocoling results of online meetings. However, this will not normally be necessary.

Microsoft Stream Cloud Storage

Cloud recordings are disabled at our Microsoft Teams Admin Center. We will inform you about anything we want to save in advance and request your consent.

Records of meetings can be saved on the Microsoft Stream Cloud. However, this requires the users to be licensed for Microsoft Stream.

Records can also be transcribed automatically so that users' discussions will be subtitled and important contributions can be found in transcriptions. Meetings will be recorded on the Cloud and may be saved on Microsoft Stream so that they may be approved securely at users' organizations.

After being recorded, a meeting will be saved by Microsoft Stream indefinitely and can only be deleted after it is deleted by the person who recorded it.

If records are not uploaded to the data stream, they will be saved on Microsoft Team's cloud storage from which they may be downloaded for **20 days**.

Microsoft Teams currently disabled the feature for recording meetings for customers whose Microsoft Teams data is stored domestically in case Microsoft Stream is not available in the domestic data region in which the data is stored. To see in which region your Microsoft Stream data is stored, click on the "?" in the upper right corner of Microsoft Stream. Then click on "Other resources" at the bottom, then on "About Microsoft Stream" and finally on "Your data is stored in". To learn more about the regions in which Microsoft Stream saves data, see the Microsoft Stream FAQ:

<https://docs.microsoft.com/en-us/stream/faq>

Notice:

However, licensing is not necessary for records to be merely downloaded by the respective users. Such records do not have to be saved on the Microsoft Stream cloud and may also be saved on "Azure Media" for **30 days** before they will be deleted.

For further information about record management and user access, see

[Manage user data in Microsoft Stream](#) and [Permissions and privacy in Microsoft Stream](#).

Encryption

Microsoft Teams data is encrypted when transferred or idle. Microsoft uses standard technologies, such as TLS and SRTP, to encrypt data during transmissions between users' devices and Microsoft data centers and between Microsoft's data centers. This

includes messages, files (video, audio etc.), meetings and other content. Idle Group data at Microsoft data centers is also encrypted in a manner that enables organizations to decrypt this data if necessary.

Furthermore, Microsoft Teams uses TLS and MTLS to encrypt chat messages. All server-to-server traffic requires MTLS—irrespective of whether traffic is limited to the internal network or exceeds the internal network perimeter.

For further information about how Microsoft Teams encrypts data, please see: [Security and Microsoft Teams](#)

Multi-Factor Authentication

We also use multi-factor authentication. This method requires users to provide additional proof of their identity. This protects accounts from attackers seeking weak or stolen passwords.

Automated Decision-Making

Automated decision-making within the meaning of Article 22 of the General Data Protection Regulation is not used.

Legal Basis of Data Processing

Any personal data of TÜV NORD GROUP employees processed via the client, TÜV NORD Service GmbH & Co. KG, is processed on the legal basis of Article 88 of the General Data Protection Regulation pursuant to Section 26(1) of the German Federal Data Protection Act [Bundesdatenschutzgesetz] (BDSG). Any personal data that is processed in relation to the use of Microsoft Teams and not necessary for the establishment, defense or termination of an employment relationship, but essential for using Microsoft Teams is processed on the legal basis of Article 6(1)(f) or, alternatively, Article 6(1)(c) of the General Data Protection Regulation.

Our legitimate interest consist of simplifying internal communication, processing inquiries, improving efficiency and promoting cooperation across the Group and its branches. Data subject interests that must be protected and prevent the introduction/use of such services are not present. In addition, the legal basis for processing data during online meetings held as part of contractual relationships is Article 6(1)(b) of the General Data Protection Regulation.

We may also process your data on the basis of your consent under Article 6(1)(a) of the General Data Protection Regulation. This will especially be done if you use the online tool or voluntarily disclose data that is not necessary for using the online service (so-called optional information).

Data Recipients and Transfers

Personal data processed in relation to participation in online meetings will not be transferred to third parties if the data is not intended to be transferred. Please note that, like with personal meetings, content from online meetings is used to communicate information to customers, prospective customers and third parties and is therefore intended to be transferred.

The provider of Microsoft Teams will necessarily learn of the above-stated data to the extent specified in processing agreement with Microsoft.

Processing Data Outside of the European Union

Microsoft Teams is a service performed by a provider from the US.

Personal data is therefore also processed in a third country. This may present latent risks for users because, e.g., data subject rights may be difficult to enforce.

2.9 Data Storage/Erasure

If the controller ends its use of Microsoft's service, the corresponding personal data will be erased between 90 and 180 days after the suspension of the use of the service.

We erase personal data when its storage is no longer necessary. Storage may be necessary if the data is still needed for the performance of a contract or reviewing, granting or defending against warranty or guarantee claims. In this case, Microsoft must comply with the request of TÜV NORD Service GmbH & Co. KG (Group administrator).

For further information about the storage of personal data on Microsoft Teams, please see:

<https://docs.microsoft.com/en-us/microsoftteams/teams-privacy>

You have the right of access to personal data concerning you. To obtain such access, you may contact us at any time.

The link to our contact form is provided here:

[Online Form for Safeguarding Data Subject Rights](#)

If access is not requested in writing, please understand that we may require additional proof to verify your identity and that you are the person you claim to be.

In case of processing based on consent, consent may be withdrawn at any time. However, withdrawal will not affect the lawfulness of processing based on consent before its withdrawal.

Furthermore, to the extent permitted by law, you have the right to rectification, erasure and restriction of processing.

You also have the right to object to processing as provided by law. You also have a right to data portability as established under data protection law.

Finally, you have the right to lodge a complaint with a supervisory authority.

If you have any problems, complaints or questions about data protection for Microsoft's "Chief Privacy Officer" or the "EU Data Protection Officer," please contact them via Microsoft's [web form](#).

Microsoft's EU Data Protection Officer may be contacted at:

Microsoft Place
South County Business Park, Leopardstown Dublin 18, Ireland.
Telephone: +353 1 706 3117