

## Information on data protection and AI techniques

As part of the use of Microsoft 365 at Bürkert and to participate in online meetings and video conferences via

**“Microsoft Teams”**

*(German Version below)*

Please find below some information from us concerning the processing of your personal data in connection with our use of Microsoft Teams (hereinafter the “Provider”).

### 1. Who is responsible for data protection compliance?

The Bürkert company that employs you or with which you have a contract is responsible for data processing.

You can find an overview of the respective companies with their addresses here

#### [Companies](#)

You can reach our data protection contact and our data protection officer at the following email address:

[dataprivacy@burkert.com](mailto:dataprivacy@burkert.com)

### 2. Which data do we process, for what purposes, for how long and on what legal basis?

Microsoft 365 offers a collaboration platform that combines chat, meetings, appointments and emails. Office products are used to create business documents in all processing processes at Bürkert. Some Microsoft 365 applications allow you to create creative content.

Please see the table in Annex I for information on which applications we use for which purposes, with which data categories and for how long we use the data in each application.

Various data types are processed in conjunction with the use of this service. The extent of the data also depends on what data you provide when using or participating in our Microsoft applications, e.g. what content your emails contain or what type of use or collaboration the available applications are used for.

Microsoft 365 is a collaboration platform from **Microsoft Corporation**

One Microsoft Way, Redmond, WA 98052-6399, USA. We have concluded a Data Privacy Agreement with Microsoft to protect your data.

You can read more about how Microsoft uses your data here:

<https://privacy.microsoft.com/de-DE/privacystatement>

You can find transparent information about the various Microsoft applications here:

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Office365>

### 3. Information about meeting recordings

**As a matter of principle, records of meetings shall not be made by us. In certain cases, i.e. for training or specific “talk sessions”, it may be necessary to record the meeting. Participants will be informed of this prior to the Online Meeting. Participants will have the opportunity to disable their own video image or even refrain from participating in the chat.**

Irrespective of the case of a recording, where applicable you will have the opportunity to use the chat, question or query functions during an Online Meeting. In this respect, the text entered by you will be

processed to be featured in an Online Meeting and, where applicable, recorded. In order to feature video and playback audio, relevant data from your end device microphone and that from any possible video camera will be processed during the meeting. You can switch off or mute the camera or microphone yourself at any time via the application.

To participate in an Online Meeting or to enter a “meeting room”, you will be required to provide the necessary minimum information.

The legal basis for data processing when organizing and conducting “online meetings” is our contract, insofar as the meetings are held within the framework of contractual relationships.

In the absence of a contractual relationship, or in the event that conducting a meeting is not essentially required to fulfil the contract, the legal basis shall be our legitimate interest. In this case, effective communication through Online Meetings is in our legitimate interest.

Insofar as participation in an Online Meeting occurs within the scope of training activities, we have obtained your written consent to this in advance. The legal basis shall then be this consent.

If you are registered with a Provider, then further data concerning Online Meetings will be saved (meeting metadata, telephone dial-in data, questions and responses during webinars, query functions during webinars).

#### **4. Who the data is transmitted to (recipient categories)**

Personal data will generally not be passed on to third parties unless specifically intended for this purpose.

##### Further recipients:

As our data processor, Microsoft necessarily receives knowledge of the data listed in Annex I, insofar as this is provided for in our data processing agreement.

#### **5. How long do we store your data?**

We will delete your personal data when there is no longer a need for further storage. In particular, there may be a need if the data is still required for the purposes of rendering contractual services. In the case of legal storage obligations, deletion shall only be considered at the end of the respective storage obligation.

Information about our deletion routines within Microsoft applications can be found in Annex I.

#### **6. Data transmission to third countries:**

The service provider is based in the USA. Personal data is thus also processed in a third country. We have concluded an order processing contract with the Provider which complies with the requirements of Article 28 of the GDPR. An appropriate level of data protection is guaranteed by the conclusion of the so-called EU standard contractual clauses and the certification of Microsoft under the EU adequacy decision.

#### **7. Rights of data subjects, right of complaint**

You have the right to request information about the personal data stored about you and to request correction. You have the right to request the deletion of your data if its processing is no longer necessary and the other requirements of the GDPR for deletion are met or to request the restriction of processing or to object to the processing as well as the right to data portability; to complain to the data protection supervisory authority if you believe that the processing of your personal data violates the GDPR.

## **8. Mandatory information under the AI Regulation**

Some of the applications included in Microsoft 365 contain AI techniques. You can find this in the table in Annex I.

Here you can find information about Microsoft's AI standards and Microsoft's Transparency Report:

<https://blogs.microsoft.com/on-the-issues/2025/01/15/innovating-in-line-with-the-european-unions-ai-act/>

## **9. Obligation to provide data**

The data described in Annex I, which is collected systemically, is automatically collected when using the respective communication tools or the mentioned apps. The use of the applications or communication tools listed in Annex I is not possible without the collection of the systemic minimum data processing. Additional user data (information about persons, work results, business data) is provided voluntarily by the respective user.

## **10. Automated decision-making, profiling**

Automated decision-making and profiling do not take place.

*As of 15.04.2025*

## Annex I

Name of the application	Purpose of processing	Legal basis	Categories of personal data	Categories of data subjects	Duration of storage	Contains AI (see section 8.)
Entra ID	Identity and access management: authentication, authorization	for the implementation of the employment relationship or contract, otherwise based on legitimate interest	Identity data (e.g. name, username, email address), contact information, job information (e.g. position, department) and login information. Address data Login data Account data Employee data Position data Contact details	Employees, consumer, customers, suppliers	Until termination of the contractual relationship, deletion 30 days after withdrawal, in the USA after 90 days	no
Intune	Device management: Management and protection of mobile devices	for the implementation of the employment relationship or contract, otherwise based on legitimate interest	Device information (e.g. device ID, operating system), user information (e.g. name, email address), location data (for company devices), application usage data. Login data Account data Employee data Usage data... Usage history Device information	Employees, external user	Until the end of the device's lifespan	no
Bookings	Appointment management: booking appointments and schedule management	based on legitimate interest	Contact information (e.g. name, email address, telephone number), calendar and appointment information. Contact details User data: Usage data... Calendar and appointment data	Employees, consumer, customers, suppliers	Customer data is stored in backup for 10 years. (Note: because storage in backup)	no
Dynamics	Customer relationship management: Managing customer relationships and sales data	based on legitimate interest	Customer and contact data, transaction data, communication data (e.g. emails, calls). Address data Account data Bank details / billing information Employee data	Employees, consumer, customers, interested parties, suppliers	Data from customers, suppliers and interested parties will be deleted depending on	no (except Sales Copilot)

			Contract data Contact details Communication data		the existence of the respective contractual relationship.	
Forms	Survey creation: Collecting data through surveys and forms	based on legitimate interest	Responses to surveys and forms that may contain personal data (e.g. name, email address, feedback). User data: Usage data... Communication data Responses to surveys and forms	Employees, consumers, customers, suppliers	Until termination of the contractual relationship, deletion 30 days after withdrawal, in the USA after 90 days. Content shared by users is stored until it is deleted by the user or recipient.	no
Task / ToDo	Task management: task management and prioritization	based on legitimate interest	Task and note data, which may contain personal information (e.g. names, reminders). User data: Usage data/logs of timestamps Task and note data Content created in the ToDo	Employees	Until termination of the contractual relationship, deletion 30 days after withdrawal, in the USA after 90 days. Content shared by users is stored until it is deleted by the user or recipient.	no

Whiteboard	Collaboration: Creation and management of visual content	for the implementation of the employment relationship or contract, otherwise based on legitimate interest	Content created on the whiteboard, including text, drawings, and inserted documents that may contain personal information (e.g., names, reminders). User data: name, email Technical data: IP addresses, device IDs, browser information, data visualizations Communication data: Content created on the whiteboard	Employees, external participants	Until termination of the contractual relationship, deletion 30 days after withdrawal, in the USA after 90 days. Content shared by users is stored until it is deleted by the user or recipient.	no
Stream	Video hosting: storage and management of videos	for the implementation of the employment relationship or contract, otherwise based on legitimate interest	Video content that may contain personal information (e.g. recordings of meetings). Image data / video data (if shared by users) Technical data: IP addresses, device IDs, browser information, data visualizations	Employees, external participants	The user will be deleted after termination of the contractual relationship, usually 30 days after termination, in the USA after 90 days. Content shared by users remains stored until deleted by the user or recipient.	no
Power BI	Data analysis: Creating reports and dashboards	based on legitimate interest	Data visualizations that may contain personal data (e.g. reports, dashboards). User data: Name, email address, login information, Financial data: bank account details, transaction data Professional data: job ti-	Employees	The user will be deleted after termination of the contractual relationship, usually 30 days after termination, in the USA after	no

			<p>tle, department, working hours</p> <p>Technical data: IP addresses, device IDs, browser information, Data visualizations</p>		<p>90 days. Content shared by users remains stored until deleted by the user or recipient.</p>	
Loop	<p>Real-time collaboration: Create and edit content in real time</p>	<p>for the implementation of the employment relationship or contract, otherwise based on legitimate interest</p>	<p>Collaborative content that may contain personal information (e.g. names, content timestamps). Usage data... Collaborative content Content that documents people in the loop</p>	Employees	<p>The user will be deleted after termination of the contractual relationship, usually 30 days after termination, in the USA after 90 days. Content shared by users remains stored until deleted by the user or recipient.</p>	no
Consent for employee photos	<p>Obtaining consent: Use of images for marketing and communication</p>	<p>based on the user's consent</p>	<p>Images: Image files, consent forms</p>	Employees	<p>Until consent is revoked or the employee leaves.</p>	no
Sharepoint Online (Basis)	<p>Data storage and programmable logic controller</p>	<p>for the implementation of the employment relationship or contract, otherwise based on legitimate interest</p>	<p>Documents and files that may contain personal information. User data: name, email address, login information Technical data: IP addresses, device IDs, browser information Log data: telemetry and diagnostic data Activity logs Usage data... Documents and files</p>	Employees, external participants	<p>The user will be deleted after termination of the contractual relationship, usually 30 days after termination, in the USA after 90 days. Content shared by</p>	

					users re- mains stored until deleted by the user or recipient.	
OneDrive	Data storage and programmable logic controller	for the implementation of the employment relationship or contract, otherwise based on legitimate interest	Documents and files that may contain personal information. User data: name, email address, login information Log data: telemetry and diagnostic data Activity logs Technical data: IP addresses, device IDs, browser information Usage data... Documents and files	Employees, applicants, consumer, customers, interested parties, suppliers	The user will be deleted after termination of the contractual relationship, usually 30 days after termination, in the USA after 90 days. Content shared by users remains stored until deleted by the user or recipient.	no
Outlook (Basis)		for the implementation of the employment relationship or contract, otherwise based on legitimate interest	Calendar and contact details User data: name, email address, login information Usage data... Log data: telemetry and diagnostic data Activity logs Calendar and contact details Technical data: IP addresses, device IDs, browser information	Employees, applicants, consumer, customers, interested parties, suppliers	The user will be deleted after termination of the contractual relationship, usually 30 days after termination, in the USA after 90 days. Content shared by users remains stored until deleted by the user or recipient.	no

teams	Communication and collaboration platform	for the implementation of the employment relationship or contract, otherwise based on legitimate interest	Chat messages, video conferences, files and calendar data. User data: name, email address, login information Usage data... Log data: telemetry and diagnostic data Activity logs Calendar and contact details Technical data: IP addresses, device IDs, browser information Chat messages and video conferences	Employees, applicants, consumer, customers, interested parties, suppliers	The user will be deleted after termination of the contractual relationship, usually 30 days after termination, in the USA after 90 days. Content shared by users remains stored until deleted by the user or recipient.	no (except M365 Copilot)
Office	Office apps for editing Office data	for the implementation of the employment relationship or contract	Documents, spreadsheets and presentations that may contain personal information. Usage data... Documents, tables and presentations Content created by users	Employees, applicants, consumer, customers, interested parties, suppliers	The user will be deleted after termination of the contractual relationship, usually 30 days after termination, in the USA after 90 days. Content shared by users remains stored until deleted by the user or recipient.	no (except M365 Copilot)
Authenticator	Tool for multi-factor authentication at MS	for the implementation of the employment relationship or contract, otherwise based on legitimate interest	Identity data: username, email Login data Safety information	Employees	Log data is stored by the system for 180 days.	no

Ex- change Online (Basic)	email Sent In- frastructure	for the imple- mentation of the employment re- lationship or con- tract	User data: name, email address, login infor- mation Usage data... Log data: telemetry and diagnostic data Activity logs Calendar and contact details Technical data: IP ad- resses, device IDs, browser information Calendar and contact details	Employ- ees, appli- cants, con- sumer, custom- ers, inter- ested par- ties, sup- pliers	The user will be de- leted after termination of the con- tractual re- lationship, usually 30 days after termina- tion, in the USA after 90 days. Content shared by users re- mains stored until deleted by the user or recipient.	no
Backup	Data backup	Ensuring data availability and secure data stor- age over a long period of time.	User data: Name, email address, login infor- mation, Content created or pro- vided by the user	Employ- ees, appli- cants, con- sumer, custom- ers, inter- ested par- ties, sup- pliers	The user can delete user-gener- ated data in his applica- tion/fronte nd at any time and then no longer has access to it. Backup stores for 10 years, access con- trol only for IT adminis- trators, en- ryption and other TOMs	no
Copilot (basic)	AI/productiv- ity support tool.	for the imple- mentation of the employment re- lationship or con- tract, otherwise based on legiti- mate interest	Custom applications that can process per- sonal data.	Employees	All user data is de- leted by the system af- ter 180 days.	yes

Audit-Log	The audit log is a key element for maintenance, troubleshooting and protecting your M365 infrastructure.	Due to the legitimate interest in carrying out maintenance and troubleshooting as well as error correction in order to ensure the error-free usability and availability of the application.	Log data that tracks activities and changes within the Microsoft 365 environment Log data: telemetry and diagnostic data Activity logs User data: name, email address, login information Technical data: IP addresses Device IDs	Employees, external network participants	All log files/protocols are deleted by the system after 180 days.	no
Voice assistant	The voice assistant is used primarily to efficiently design the workflow. In some cases (e.g. For people with visual impairment, the voice assistant would be an important support for everyday work.	based on the user's consent	User data: name, email address, login information Technical data: IP addresses, device IDs	Employees	Users can delete their voice recordings using the activity history settings in their Microsoft account. This includes the options to delete individual or all recordings.	yes
Power Apps	Tool for creating low-code applications or workflows	for the implementation of the employment relationship or contract, otherwise based on legitimate interest	Custom applications that can process personal data	Employees, external	The user will be deleted after termination of the contractual relationship, usually 30 days after termination, in the USA after 90 days. Content shared by users remains until deleted by the user or recipient.	no

As of 15.04.2025

