

Terms of Use for the use of Microsoft Office 365 Components at Fraunhofer-Gesellschaft by External Parties and Data Protection Information

Last revised 24 March 2020

As a Fraunhofer project or business partner, you are invited to use Office 365 components in collaborating with Fraunhofer-Gesellschaft. Fraunhofer-Gesellschaft makes these components available with the assistance of Microsoft.

For your own protection, but also for the protection of the employees of Fraunhofer-Gesellschaft and in order to comply with laws, company-wide agreements and other regulations, the following binding Terms of Use (hereinafter Part I) shall apply. These Terms of Use shall become a component of the contractual relationship between Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastrasse 27c, 80686 Munich and you or, if applicable, the company or organization represented by you.

Acceptance of the invitation and the use of the Microsoft Office 365 components made available shall be deemed a binding declaration of acceptance of these Terms of Use without deviations. If you are acting for a company or an organization that cooperates with Fraunhofer-Gesellschaft, you further confirm thereby that you are authorized to accept the Terms of Use without changes.

If this is not possible or if you have questions, please get in touch with your contact at Fraunhofer-Gesellschaft prior to use.

Aside from that, we wish to provide you with information with respect to the processing of your personal data when using Microsoft Office 365 components pursuant to Article 13 General Data Protection Regulation (hereinafter Part II).

Table of contents

I. Terms of Use for Microsoft Office 365 components	11
1. Basic rules for the use of O365 Components	
1.1 Purpose	11
1.2 Need-to-know principle	11
1.3 Confidentiality and information classification	11
1.4 Intellectual property	11
1.5 Termination	12
1.6 Liability	12
2. Regulations on information security	
2.1 Data security and protection of confidentiality	12
2.2 Passwords	12
2.3 Protection from spam and viruses, logging and control	12
2.4 Mobile devices	13
2.5 Availability	13
2.6 Reporting requirements	13
3. Special conditions for the use of the O365 Component "Microsoft Teams"	
3.1 Transparency	13
3.2 Camera function	13
3.3 Participation	13
3.4 Recording of a team conference	13
II. Data protection information pursuant to Article 13 GDPR	14
Essential data protection information for the operation of Microsoft Office 365	14

I. Terms of Use for Microsoft Office 365 components

The following Terms of Use of Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastraße 27c, 80686 Munich (hereinafter “Fraunhofer-Gesellschaft”) shall apply to all persons who are not employees of Fraunhofer-Gesellschaft within the meaning of the Betriebsverfassungsgesetz [Works Constitution Act] (hereinafter “External Parties” or “External Users”) when using Microsoft Office 365 components that Fraunhofer-Gesellschaft makes available for collaboration (hereinafter “O365 Components”).

1. Basic rules for the use of O365 Components

1.1 Purpose

Fraunhofer-Gesellschaft makes all O365 Components available exclusively for the purpose of business collaboration in connection with projects, task orders and the performance of contractual obligations in the relationship with External Parties. The same applies to the contents made available by means of the Components, such as research data, documents, presentations, etc. Use of the O365 Components and contents for any other purposes is prohibited. In particular, use of the O365 Components and contents for personal purposes, the transfer of contents to personal devices or personal storage devices that are not subject to the exclusive control of the External Party’s company or organization as well as the use of information for the analysis of the performance or conduct of employees of Fraunhofer-Gesellschaft is prohibited. Personal and social data of employees of Fraunhofer-Gesellschaft, to the extent that these are accessible to External Parties, must not be stored in O365 storage files.

1.2 Need-to-know principle

All processing of contents in and from O365 Components shall be subject to the necessity principle. Even within a joint team contents may be forwarded only to those persons who must be made aware of them to perform their duties.

The forwarding of contents from O365 Components to persons external to Fraunhofer outside a team (third parties) shall require the prior explicit consent of Fraunhofer-Gesellschaft.

1.3 Confidentiality and information classification

For all contents made available through O365 Components and for all information that can be derived from the use, the confidentiality provisions existing between Fraunhofer-Gesellschaft and the External Party shall apply accordingly. For the handling of contents and information from the O365 Components the requirements of the project management or of the party issuing the invitation are to be complied with, particularly requirements concerning the handling and forwarding of contents classified as confidential.

1.4 Intellectual property

External Parties may not assert or apply for any patent, trademark or other rights to contents from O365 Components, for themselves or for third parties, unless the proprietor of the rights has granted

O365: Nutzungsbedingungen und Datenschutzinformationen für Externe

its prior written consent or such entitlement is governed by the contract underlying the use, e.g., in a task contract or a project contract.

1.5 Termination

The provision of the O365 Components may be terminated at any time by Fraunhofer-Gesellschaft. The External Party shall then be given the opportunity to receive data belonging to him.

1.6 Liability

Fraunhofer-Gesellschaft shall be liable for pecuniary damage in connection with the use of the O365 Components only in the event of intent and gross negligence. In the event of a negligent breach of an essential contractual obligation, Fraunhofer-Gesellschaft's liability shall be limited to typically foreseeable damage. These exclusions and limitations of liability shall also apply to all organs, vicarious agents and employees of Fraunhofer-Gesellschaft. They shall not apply in the event of injury to life, limb or health.

2. Regulations on information security

2.1 Data security and protection of confidentiality

Access by unauthorized persons to the O365 Components made available by Fraunhofer-Gesellschaft and to the data processed (and stored) with them is to be prevented by means of risk-appropriate technical and organizational measures within the meaning of Article 32 General Data Protection Regulation (GDPR). In implementing the measures the state of the art is to be taken into account. Access must be blocked even in the case of a short absence; in the case of a longer absence the computer must be shut down.

2.2 Passwords

Passwords (and PINs) must not be given to unauthorized persons, i.e., to persons for whom access to O365 Components is not required in order to perform a project, a task order or a contractual business relationship. Passwords selected must be secure in accordance with the state of the art and are to be kept secret. Passwords for access to O365 Components are not to be reused for other purposes.

2.3 Protection from spam and viruses, logging and control

Emails and other data suspected of containing malware, viruses or spam may be quarantined at the discretion of Fraunhofer-Gesellschaft or centrally and automatically deleted.

For the purposes of system administration, i.e., particularly for the analysis and remedying of system problems, for ensuring IT, operational and information security and for maintenance support, there may be personal evaluations of data that were collected in using the O365 Components. This shall also apply to the prevention of cyber attacks. In certain cases there may also be a forensic examination of the hardware used. Data from the operating system, from components related to the operating system, traffic data from internet services and tool-related data may be logged for these purposes and may also include personally identifiable data.

O365: Nutzungsbedingungen und Datenschutzinformationen für Externe

2.4 Mobile devices

The use of O365 Components via notebooks, smartphones and tablets requires separate security precautions. Mobile devices are not to be left unsupervised at freely accessible locations. If the IT Department of the External Party has not specified and installed security settings, the External Party must do so himself. Entering a PIN or password and their activation when the mobile device is not used is to be set up, and if a wrong code is entered multiple times, then (for smartphones and tablets and to the extent possible) further log-in processes must be blocked or delayed. Company data of Fraunhofer-Gesellschaft, particularly address books and emails, must not be stored with other third-party providers or synchronized via other clouds without special permission of the Fraunhofer project manager. In the event that a device is lost Fraunhofer-Gesellschaft is to be informed immediately if there is a risk that access data or Fraunhofer-Gesellschaft data may fall into the hands of unauthorized persons. If possible, remote deletion is to be performed and a theft/loss report is to be filed.

2.5 Availability

Fraunhofer-Gesellschaft does not guarantee any specific availability of the O365 Components or the data processed (and stored) with them.

2.6 Reporting requirements

Indications of violations of data protection, abuse, security-related weak points or security-related events (such as unauthorized data access or release) are to be reported by External Parties to the respective contact at Fraunhofer-Gesellschaft without delay.

3. Special conditions for the use of the O365 Component “Microsoft Teams”

3.1 Transparency

For all members of a team room, both for employees of Fraunhofer-Gesellschaft and for External Parties, there is transparency with regard to the other members of a team room. In particular, it is forbidden to give the personal access data to a team room to other persons without authorization or to allow other persons to secretly take part in a team conference, particularly a telephone or video conference. The functionality of the video conference systems used shall be designed such that the respective participant can see which video and audio data are recorded, transferred and stored.

3.2 Camera function

Based on internal Fraunhofer rules, employees of Fraunhofer-Gesellschaft are not obliged to use the camera function when participating in video conferences, nor can this be required by External Parties.

3.3 Participation

Based on internal Fraunhofer rules, employees of Fraunhofer-Gesellschaft have the right to have their concerns regarding the video and audio data concerning them respected by other participants and by External Parties. Employees of Fraunhofer-Gesellschaft may therefore, for example, also (co-)determine whether the local system should allow automatic dial-in from outside, whether the local cameras can be controlled by the conference partner, and whether and how application sharing is to take place.

3.4 Recording of a team conference

Image and sound recordings (including snapshots) may be made only with the consent of the participants. The purpose, along with the consent of the participants to the recording, shall

O365: Nutzungsbedingungen und Datenschutzinformationen für Externe

be documented within the recording. Each participant shall have the right to receive a copy of the recording.

Agreement shall be reached among the participants concerning the use of video and audio data stored within the scope of the stated purpose. Should no agreement be reached in this matter, the data shall be deleted immediately after the conference.

Should a recording be altered for any purpose beyond quality improvement, all participants identifiable in the final version must give their consent to this version and to any amended purpose of the recording.

Unless a deletion date has been determined as part of the purpose of the recording, the recording and all copies are to be deleted no later than 12 months after the end of the recording. Upon request the External Party shall confirm to Fraunhofer-Gesellschaft the deletion of his own permissible recordings.

Any provision of video and sound recordings to persons outside a team (External Parties or employees of Fraunhofer-Gesellschaft) shall require the documented consent of the participants in the recording.

II. Data protection information pursuant to Article 13 GDPR

Below you will find information pursuant to Article 13 General Data Protection Regulation (GDPR) concerning the processing of your personal data when using the Microsoft Office 365 Components. The information takes into account the material facts that follow from the operating concept in the Microsoft Cloud. Additional data protection information on Microsoft Office 365 may be found on Microsoft's [websites](#).

Essential data protection information for the operation of Microsoft Office 365

- Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastrasse 27c, 80686 Munich, tel. +49 89 1205-0, fax +49 89 1205-7531, info@zv.fraunhofer.de, is responsible vis-à-vis external users for the operation in matters of data protection law. Microsoft Ireland Operations Ltd. from Dublin is a contractual partner of Fraunhofer-Gesellschaft and operates Microsoft Office 365 as a processor for Fraunhofer-Gesellschaft within the meaning of Article 28 GDPR.

O365: Nutzungsbedingungen und Datenschutzinformationen für Externe

- The data protection officer at Fraunhofer-Gesellschaft may be reached at the above-cited address, in care of the data protection officer or at datenschutz@zv.fraunhofer.de.
- The processing of data with Microsoft Office 365, including data storage, takes place in the Microsoft Cloud, in computer centers located in Europe.
- The overall purposes of the data processing are primarily the use (including mobile use) of a collaboration platform that is certified and as functionally comprehensive as possible in a uniform IT ecosystem with principals and clients. The purposes of the processing by individual O365 Components follow from the functions of the respective O365 Components made available to External Parties.
- As a rule, the legal bases within the meaning of Article 6 GDPR for the data processing of External Parties' personal data by the O365 Components made available by Fraunhofer-Gesellschaft are Article 6 (1) lit. b GDPR (performance of a contract) and Article 6 (1) lit. f GDPR (legitimate interests). This does not preclude that data processing may also take place on other legal bases, for example, based on consents given to Fraunhofer-Gesellschaft.
- It is not intended to transfer personal data based on the operation of Microsoft Office 365 to a third country. In particular, there is no storage of data in third countries. However, in compliance with the general regulations (e.g., rules of export control) data may be customarily sent to project partners or principals in third countries or on trips to third countries may be retrieved from there.
- According to the Microsoft operating concept, disruptions should for the most part be remedied automatically. In individual cases, support staff of Microsoft or of Microsoft's subcontractors may have to be called in. In extremely rare cases, downstream Microsoft support engineers may also have to access so-called personal client data on Fraunhofer-Gesellschaft storage areas, for example, to repair mailbox databases. In such cases (possibly partial) awareness of personal client data cannot be ruled out. Access may take place from third countries in which there is no adequate level of data protection within the meaning of the GDPR and for which there is no adequacy decision by the EU Commission, for example, from the US. In these cases the adequate level of data protection shall be assured by means of previously agreed-upon standard data protection clauses that grant the data subjects rights similar to those in the EU. A [copy](#) of the signed standard data protection clauses is attached as Appendix 3 to the Microsoft Terms and Conditions for Online Services.
- Irrespective of the location from which client data are accessed, each such access requires the prior and explicit approval by Fraunhofer-Gesellschaft as part of the so-called Customer-Lockbox process. The approval is granted by specially authorized employees of Fraunhofer-Gesellschaft. Any access approved shall be possible only to the partial data required in the specific case, shall be time-limited and shall be logged. After the expiration of the time limit or the achievement of the purpose of the inquiry, Fraunhofer-Gesellschaft shall be informed of the access.

O365: Nutzungsbedingungen und Datenschutzinformationen für Externe

- Microsoft Office 365 also records the log data of the individual components for administrative purposes. The recording takes place centrally, in computer centers located in Europe. The access rights to these data are restrictively regulated at Fraunhofer-Gesellschaft. By default, personal log data are deleted after 90 days.
- No profiling or automated decision-making pursuant to Article 22 GDPR by Fraunhofer-Gesellschaft shall take place in the operation of Microsoft Office 365.
- Additional data protection information when using the Microsoft Office 365 component "Microsoft Teams"

In connection with using Microsoft teams (e.g. participating in a telephone or video conference) the following data may be processed:

- Access data: e.g., an individualized link through which you were invited to a conference.
- Content data: Contents of your contributions, e.g., in chats or files released by you.
- Image or sound recordings: Section 3.4 of the Terms of Use applies. Legal basis of the processing is your consent.
- Profile data: Data about yourself that your organisation or you have voluntarily released in connection with using Microsoft Teams; for example, your name or your profile photo. Profile data are used for personalization and for a more personal style of communication.
- Dial-in data: This includes, for example, the date and time of your dial-in to the conference and the time you leave it or where applicable dial-in number, name/title of the conference.
- Support /Feedback data: Information in connection with the handling of any troubleshooting tickets or feedback.
- Telemetry data: These include diagnostic data in connection with the use of the service, including the transmission quality. These data serve to improve troubleshooting, securing and updating technical service and its monitoring. The legal basis is Art. 6 (1) lit. f GDPR. Our legitimate interests are the provision of a secure and error-free communication service.

Unless otherwise specified, the processing of the data is done for the technical and content-related execution of the respective conference. The storage period of the data depends essentially on the purpose for which the respective conference is held. Log data is deleted as standard after 90 days.

In providing the service Microsoft captures certain diagnostic and service data and uses these

O365: Nutzungsbedingungen und Datenschutzinformationen für Externe

on its own authority for its own purposes. To the extent that Microsoft processes personal data in connection with its own legitimate business processes, Microsoft is the independent controller within the meaning of the GDPR for such processing. Particulars concerning the processing by Microsoft may be found at <https://docs.microsoft.com/de-de/microsoft-teams/teams-privacy>

- Rights of the data subject: You have the following rights
 - i. pursuant to Article 15 GDPR, to demand information about your personal data processed by Fraunhofer-Gesellschaft. In particular, you may request information about the purposes of the processing, the categories of personal data concerned, the categories of recipients to whom the personal data have been or will be disclosed, and the envisaged period for which the data will be stored, if possible. Moreover, you have the right to request rectification, erasure, or restriction of processing, to object to processing; the right to lodge a complaint, and to obtain information about the source of your data if they were not collected from you, as well as about the existence of automated decision-making, including profiling, and, if applicable, meaningful information about the logic involved;
 - ii. pursuant to Article 16 GDPR, to obtain the rectification of inaccurate data or the completion of your personal data stored with Fraunhofer-Gesellschaft without undue delay;
 - iii. pursuant to Article 17 GDPR, to obtain the erasure of your personal data stored with Fraunhofer-Gesellschaft, if
 - o they are no longer necessary in relation to the purposes for which they were collected or otherwise processed,
 - o you withdraw your consent on which the processing was based according to point (a) of Article 6(1) or point (a) of Article 9(2), and where there is no other legal basis for the processing,
 - o you object to the processing pursuant to Article 21(1) GDPR and there are no overriding legitimate grounds for the processing,
 - o the personal data have been unlawfully processed,
 - o the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject,
 - o the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) GDPR (child's consent).

There is no right to deletion to the extent that the processing is required

O365: Nutzungsbedingungen und Datenschutzinformationen für Externe

- o for exercising the right of freedom of expression and information,
 - o for fulfilling a legal obligation, for reasons of the public interest in the sphere of public health or for purposes of archiving in the public interest or
 - o for the establishment, exercise or defence of legal claims.
- iv. pursuant to Article 18 GDPR, to demand the restriction of the processing of your personal data, if
 - o you contest the accuracy of the data,
 - o processing is unlawful but you oppose the erasure of the personal data,
 - o if Fraunhofer-Gesellschaft no longer needs the personal data while you still require it for establishing, exercising or defending legal claims, or
 - o you objected to the processing pursuant to Article 21 GDPR.
- v. pursuant to Article 20 GDPR, to obtain your personal data that you have provided to Fraunhofer-Gesellschaft in a structured, customary and machine-readable format or to request the transmission to another controller if the processing is based on consent pursuant to Article 6 (1) lit. a GDPR or Article 9 (2) lit. a GDPR or on a contract pursuant to Article 6 (1) lit. b GDPR and the processing is done using automated processes. This right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The right referred to in Article 20 (1) GDPR shall not adversely affect the rights and freedoms of others.
- vi. pursuant to Article 7 (3) GDPR to withdraw any consent given by you to Fraunhofer-Gesellschaft at any time. The consequence of this shall be that in the future Fraunhofer-Gesellschaft must discontinue the data processing that was based on this consent if there is no other legal basis for the processing. If a request for granting consent to Microsoft is made through the Microsoft Office 365 Components used by Fraunhofer as part of the business use (for example, in connection with updates), based on agreements between Fraunhofer-Gesellschaft and Microsoft said consent shall be deemed as not having been given; and
- vii. pursuant to Article 77 GDPR, the right to lodge a complaint with a supervisory authority. Generally, you may contact the supervisory authority of your habitual residence, place of work or the registered office of Fraunhofer-Gesellschaft e.V.
- viii. Right to object: If your personal data are processed on the basis of legitimate interests pursuant to Article 6 (1) lit. f GDPR, you have the right to object to the processing of

O365: Nutzungsbedingungen und Datenschutzinformationen für Externe

your personal data pursuant to Article 21 GDPR if reasons exist for doing so that are based on your special situation.