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

Last amended 3/24/2020

As a Fraunhofer project or business partner, you will be sent an invitation to use Office 365 components in order to collaborate with the Fraunhofer Society. The Fraunhofer Society provides these components with the aid of Microsoft.

In order to protect you and the employees at the Fraunhofer Society as well as to ensure compliance with legislation, general works agreements, and other regulations, the following binding terms of use apply (Part I below). These terms of use form part of the contractual relationship between Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastraße 27c, 80686 Munich, Germany, and you or, if relevant, the company or organization that you represent.

Acceptance of the invitation and use of the Microsoft Office 365 components is regarded as a binding declaration of acceptance of these terms of use without exception. Should you be acting on behalf of a company or organization with which the Fraunhofer Society cooperates, by accepting the invitation and using the components you also confirm that you are authorized to accept the unamended terms of use.

Should this not be possible or should you have any questions, please consult your contact person at the Fraunhofer Society prior to use.

In the following we provide you with details of how your personal data is processed when using Microsoft Office 365 components as per Article 13 of the General Data Protection Regulation (GDPR) (Part II below).

Contents

I. Terms of Use for Microsoft Office 365 Components

The following terms of use of the Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastraße 27c, 80686 Munich, Germany, (referred to in the following as the "Fraunhofer Society") apply to all persons who are not employees of the Fraunhofer Society as defined by the Works Constitution Act (referred to in the following as "external parties" or "external users") in connection with the use of Microsoft Office 365 components as provided by the Fraunhofer Society for the purpose of collaboration (referred to in the following as "O365 components").

1. Basic Rules for the Use of O365 Components

1.1. Intended Purpose

The Fraunhofer Society provides all O365 components exclusively for the purpose of a business collaboration within the framework of projects, orders, and the performance of contractual obligations vis-à-vis external parties. This applies accordingly for the content provided via the components, e.g., research data, documents, presentations, etc. All and any use of the O365 components and content for other purposes is prohibited. In particular, the use of the O365 components and content for private purposes, the transfer of content to private devices and private storage systems which are not subject to the sole control of the company or the organization of the external party, and the use of information to analyze the performance or behavior of Fraunhofer Society staff is strictly prohibited. Personal and social data concerning employees at the Fraunhofer Society must not be stored in O365 repositories if the latter can be accessed by external parties.

1.2 "Need to Know" Principle

The need to know principle applies to all processing of content in and from O365 components. Within a joint team, content may only be forwarded to those persons who require this information in order to perform their duties. The forwarding of content from O365 components to persons not employed by Fraunhofer who are not in a team (third parties) requires the prior, express consent of the Fraunhofer Society.

1.3 Confidentiality and Classification of Information

The confidentiality provisions existing between the Fraunhofer Society and the external party apply accordingly for all the content made accessible via the O365 components and for all the information derived from the use thereof. The stipulations of the project management or the inviting party must be noted with regard to the use of content and information from the O365 components, especially insofar as the handling and forwarding of content classed as confidential is concerned.

1.4 Intellectual Property

External parties may not assert any patent rights, trademark rights, or other rights on content from O365 components for either themselves or third parties, unless the rights holder has given their prior written consent or if authorization is regulated in the contract upon which the usage is based, e.g., in an order or project contract.

1.5 Termination

Provision of the O365 components can be terminated by the Fraunhofer Society at any time. The external party is then given the opportunity to retrieve their data.

1.6 Liability

The Fraunhofer Society is only liable for financial losses in connection with the use of the O365 components in the case of intent and gross negligence. In the case of a negligent breach of a key contractual obligation, the liability of the Fraunhofer Society is limited to typically foreseeable damages. These liability exclusions and restrictions also apply to all institutions, vicarious agents, and staff at the Fraunhofer Society. They do not apply in the event of injury to life, limb, or health.

2. Regulations on Information Safety

2.1 Data Safety and Protection of Confidentiality

Access by unauthorized parties to the O365 components provided by the Fraunhofer Society as well as to the processed (and saved) data is to be prohibited by means of risk-appropriate technical and organizational measures as defined by Article 32 of the General Data Protection Regulation (GDPR). The state of the art must be taken into consideration when implementing such measures. Access must also be blocked even during brief periods of absence; computers must be shut down during extended periods of absence from the workstation.

2.2 Passwords

Passwords (and PINs) must not be forwarded to unauthorized persons, i.e., to persons who do not require access to O365 components in order to complete a job or a business contractual relationship. Strong passwords are to be selected based on the state of the art and are to be kept secret. Passwords used to access O365 components must not be used multiple times for other purposes.

2.3 Protection against Spam and Viruses, Logging and Control

E-mails and other data with suspected malicious code, viruses, or spam may be put into quarantine or deleted centrally and automatically at the discretion of the Fraunhofer Society.

Personal evaluations of data which arise from the use of the O365 components are possible for system administration, i.e., in particular for the analysis and rectification of system problems, to ensure IT, operational, and information safety, and to aid maintenance. This also applies to measures to prevent cyberattacks. In certain cases, a forensic examination of the hardware used is also possible. Data from the operating system, components related to operating systems, traffic data from Internet services, and tool-related data can be logged for these purposes and may contain personal data.

2.4 Mobile Terminal Devices

The use of O365 components with notebooks, smart phones, and tablets demands special safety precautions. Mobile terminal devices must not be left unsupervised in freely accessible places. If the external party's IT department has not prescribed and set safety settings, the external party must do this independently. PIN or password entry and the activation thereof

when the mobile device is not in use must be switched on. If an incorrect code is entered several times (with smartphones and tablets plus as far as possible in other cases), further login processes must be blocked or delayed. The operational data of the Fraunhofer Society, in particular address books and e-mails, must not be saved with other third-party providers or synchronized via other clouds without the separate approval of those responsible for the project at Fraunhofer. The Fraunhofer Society must be notified immediately of the loss of devices if there is a risk that access data or data from the Fraunhofer Society could fall into unauthorized hands. If possible, the data should be deleted remotely and the theft or loss must be reported.

2.5 Availability

The Fraunhofer Society does not guarantee any specific availability for O365 components or the data processed (and saved) with them.

2.6 Reporting Obligations

External parties must report any indications of data protection breaches, of misuse, of safety-relevant weaknesses, or of safety-relevant incidents (e.g., unauthorized data accesses or approvals) to the respective contact person at the Fraunhofer Society without delay.

3. Special Terms of Use for O365 Components “Microsoft Teams”

3.1 Transparency

It must be clear to all members in a team room as well as employees of the Fraunhofer Society and external parties who the other members in a team room are. In particular, it is prohibited to provide the personal access data for a team room to other parties without authorization or to allow other parties to take part in a team conference secretly, in particular a telephone or video conference. The functionality of the video conference systems used is such that the participants can see which video and audio data are recorded, transmitted, and saved.

3.2 Camera Function

Due to Fraunhofer-internal regulations, employees of the Fraunhofer Society are not obliged to use the camera function when participating in video conferences. This can also not be demanded by external parties.

3.3 Codetermination

Due to Fraunhofer-internal regulations, employees of the Fraunhofer Society can assert their right for their concerns with regard to the video and audio data to be respected by other participants and external parties. Employees at the Fraunhofer Society can therefore, for example, also codetermine with respect to external parties whether the local system should allow automatic dial-up from outside, whether conference partners should be able to control local cameras, and whether application sharing should be possible as well as what form this should take.

3.4 Team Conference Recordings

Images and sound (including snapshots) may only be recorded with the consent of those participating. The intended purpose and the consent to recording given by the participants will

be documented within the recording. Every participant has the right to receive a copy of the recording.

An agreement shall be reached between the participants as to the use of saved video and audio data within the framework of the intended use. If an agreement is not reached to this end, the data will be deleted immediately after the conference.

If a recording is changed for a reason other than for improving quality, all participants who can be identified in the final version must agree to this version and consent to the changed intended purpose of the recording if relevant.

If a deletion deadline was not specified within the scope of the intended purpose of the recording, the recording and all copies thereof are to be deleted 12 months after the end of the recording at the latest. The external party shall confirm the deletion of its own, approved recordings to the Fraunhofer Society upon request.

The provision of video and sound recordings to persons outside of a team (external parties or staff at the Fraunhofer Society) requires the documented consent of the recorded parties.

II. Data Protection Information as per Article 13 of the GDPR

In the following, we provide you with details of how your personal data is processed as per Article 13 of the General Data Protection Regulation when using the Microsoft Office 365 components provided by the Fraunhofer Society. This information takes into account the key circumstances which result from the Microsoft Cloud operating concept. Further data protection information on Microsoft Office 365 can be found on the Microsoft websites.

Key Data Protection Information for Operating Microsoft Office 365

- The Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Hansastraße 27c, 80686 Munich, Germany, Telephone +49 89 1205-0, Fax +49 89 1205-7531, info@zv.fraunhofer.de, is responsible for data protection vis-à-vis external users. The contractual partner of the Fraunhofer Society is Microsoft Ireland Operations Ltd. from Dublin, Ireland, which operates Microsoft Office 365 as the processor as defined by Article 28 of the GDPR for the Fraunhofer Society.
- The data protection officer at the Fraunhofer Society can be contacted at the above address, for the attention of the data protection officer, or at datenschutz@zv.fraunhofer.de.
- Data from Microsoft Office 365 is processed and stored in the Microsoft cloud in data centers in Europe.
- The overarching purposes of data processing are, in particular, the use (including mobile) of a functional and certified collaboration platform which is as comprehensive as possible in a uniform IT ecosystem with clients and customers. The purposes of processing by the individual O365 components result from the functions of the respective O365 components which have been provided to external parties.
- The legal basis as defined by Article 6 of the GDPR on the processing of the personal data from external parties by the O365 components provided by the Fraunhofer Society is, as a

rule, Article 6 1. (b) of the GDPR (performance of contract) and Article 6 1. (f) of the GDPR (legitimate interests). This does not rule out the possibility of data being processed on other legal bases, for example if consent is granted to the Fraunhofer Society.

- It is not intended to transfer personal data to a third country for the operation of Microsoft Office 365. In particular, no data is stored in third countries. Subject to compliance with the general rules (e.g., export control regulations), data can, however, be sent to project partners or clients in third countries as normal or, when traveling to third countries, be called up from there.
- Based on the Microsoft operational concept, faults should, by and large, be remedied automatically. In individual cases, it may be necessary to consult support staff from Microsoft or from Microsoft subcontractors. In extremely rare cases, it may be necessary for downstream Microsoft support engineers to access personal customer data in storage areas at the Fraunhofer Society in order, for example, to repair mailbox databases. To this end, it cannot be ruled out that personal customer data may (also in part) come to their knowledge. Access may also be from third countries where the data protection level as defined by the GDPR is insufficient and for which there is no adequacy decision from the EU Commission, for example from the USA. In such cases, adequate data protection is ensured in advance by means of agreed standard data protection clauses which provide those affected with similar rights to within the EU. A copy of the signed standard data protection clauses is attached to the Microsoft provisions for online services as Appendix 3.
- Irrespective of from where the customer data is accessed, any such access requires prior and explicit approval of the Fraunhofer Society within the scope of the Customer Lockbox procedure. Approval is granted by specially authorized staff at the Fraunhofer Society. Every approved access is only for the partial data which is required for the specific case, and this is limited in time and logged. On expiry of the time limit or once the purpose of the query has been satisfied, the Fraunhofer Society will be notified of the access.
- Microsoft Office 365 also logs all the log data of the individual components for administration purposes. Logging is performed centrally in the data centers in Europe. Access rights to these data are regulated restrictively by the Fraunhofer Society. Personal log data are deleted after 90 days as standard.
- The Fraunhofer Society performs neither profiling nor automated decision-making as per Article 22 of the GDPR in connection with the operation of Microsoft Office 365.
- Rights of those affected: In accordance with

  i. Article 15 of the GDPR, you have the right to request your personal data as processed by the Fraunhofer Society. In particular, you can demand information on the purposes of processing, the categories of personal data concerned, the recipients or categories of recipient to whom the personal data have been or will be disclosed, where possible, the envisaged period for which the personal data will be stored, the existence of the right to rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing, the right to lodge a complaint with a supervisory authority, where the personal data are not collected from you, any

available information as to their source, the existence of automated decision-making, including profiling, and, if relevant, meaningful information on the details thereof;

ii. Article 16 of the GDPR, you have the right to obtain without undue delay the rectification of inaccurate personal data concerning you as stored by the Fraunhofer Society or to demand the completion of such data;

iii. Article 17 of the GDPR, you have the right to obtain the erasure of your personal data as stored by the Fraunhofer Society if:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- you withdraw the consent on which the processing is based according to Article 6 1. (a), or Article 9 2. (a), and where there is no other legal ground for the processing;
- you object to the processing pursuant to Article 21 1. and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- 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;
- the personal data have been collected in relation to the offer of information society services referred to in Article 8 1. of the GDPR (child's consent).

The right to erasure cannot be asserted to the extent that processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation, for reasons of public interest in the area of public health, or for archiving purposes in the public interest; or
- for the establishment, exercise, or defense of legal claims;

iv. Article 18 of the GDPR, you have the right to obtain restriction of processing where one of the following applies:

- the accuracy of the personal data is contested;
- the processing is unlawful but you oppose its erasure;
- the Fraunhofer Society no longer needs the data but it is required by you for the establishment, exercise, or defense of legal claims; or
- you have asserted your right to object processing as per Article 21 of the GDPR;

v. Article 20 of the GDPR, you have the right to receive your personal data which you provided to the Fraunhofer Society in a structured, commonly used, and machine-readable format and have the right to transmit those data to another data controller subject to consent as per Article 6 1. (a) of the GDPR, Article 9 2. a) of the GDPR, or on the basis of a

contract as per Article 6 1. (b) of the GDPR and the processing is carried out by automated means. That 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. This right shall not adversely affect the rights and freedoms of others;

vi. Article 7 3. of the GDPR, you have the right to withdraw any consent granted to the Fraunhofer Society from the Fraunhofer Society at any time. As a consequence thereof, Fraunhofer Society may no longer continue processing the data for which consent has been granted in the future if there is no other legal basis for this. Should there be a request to provide consent to Microsoft for commercial use in connection with the Microsoft Office 365 components used by Fraunhofer (e.g., within the scope of updates), this consent shall not be regarded as granted on the basis of the agreements between the Fraunhofer Society and Microsoft and;

vii. Article 77 of the GDPR, you have the right to lodge a complaint with a supervisory authority. As a rule, you have the right to consult the supervisory authority in your habitual residence, place of work, or the registered office of the Fraunhofer-Gesellschaft e.V.

viii. Right to object: If your personal data is processed on the basis of legitimate interests as per Article 6 1. (f) of the GDPR, you shall have the right to object to the processing of your personal data as per Article 21 of the GDPR should there be reasons for this on the basis of your personal situation.