

Fabasphere

Data Processing Agreement for Public Cloud/Government Cloud Operating Models

Valid from January 1st, 2026

Public

Copyright © Fabasphere GmbH, 2025. All rights reserved.

All hardware and software names used are registered trade names and/or registered trademarks of the respective manufacturers.

These documents are public. No rights to our software or our professional services, or results of our professional services, or other protected rights can be based on the handing over and presentation of these documents.

Contractual partners

This agreement on data processing is concluded between the contracting parties in accordance with the CSA information sheet.

1. Preliminary remarks and obligation to comply

- 1.1. The following provisions shall apply to all data processing services within the meaning of Article 28 of the General Data Protection Regulation (EU) 2016/679 (hereinafter referred to as the "GDPR") and/or the applicable national regulations that the Contractor may fulfill for the client (hereinafter also referred to as "Customer"). This includes all activities connected with this agreement and during which employees of the Contractor or third parties commissioned by the Contractor may come into contact with the Customer's personal data.
- 1.2. The Customer and the Contractor undertake to comply with the relevant data protection laws with regard to the data to be processed.
- 1.3. Terms that are not explicitly defined in this agreement are subject to the definition provided in the GDPR or the respective national regulations.

2. Subject matter/term of this contract; Scope/type/purpose of data processing, types of data and the group of data subjects

- 2.1. In accordance with the GDPR and national regulations, the Contractor will process personal data on behalf of and following written documentary instructions from the Customer, pursuant to the Cloud Service Agreement (hereinafter "Main Contract" or "CSA") concluded between both parties and in accordance with this agreement.

The most recent version of the CSA can be viewed online at the website listed in the CSA Information Sheet under "Link to Basis of the Contract".

The activities affected, as well as the scope and type of data processing, are either specified in the description of services in the CSA or will result from instructions from the Customer given at a later date. The Contractor requests information (contact details) that is necessary and useful for conducting business transactions with the interested party as a Customer and activating the Customer as a user on the basis of this information. The description of this contact data can be found in the "Contractual Basis" and "Performance Characteristics Data Security" sections of the CSA information sheet.

- 2.2. Within the scope of this agreement, the Customer is solely responsible for adhering to the legal provisions of data protection legislation, particularly with regard to the permissibility of data processing and data usage within the framework of this agreement, as well as protecting the rights of data subjects. The Customer is solely responsible for informing data subjects that their data is collected, processed and used, and informing them of the purpose of this. The Customer will ensure that data subjects are informed of any option they have to withdraw.
- 2.3. The term of this agreement shall be governed by the term of the CSA, unless further obligations arise from the following provisions. Data confidentiality shall continue to apply even after termination of this agreement, regardless of the legal grounds for such termination.
- 2.4. The Contractor shall process the following personal data on behalf of the Customer:
 - a) Contact details of the Customer.

- b) The user data shall remain solely within the Customer's control and the Contractor shall not know the content of this information, nor shall they have direct access to it.

The definition and the differences between contact details and user details are provided in "Performance Characteristics Data Security".

- 2.5. The purpose of the data processing is for the Contractor to complete the tasks specified in the service description in the CSA or to follow the instructions given by the Customer.

From the Customer's perspective, the categories of data subjects are their clients, prospective clients, employees, applicants, suppliers, contractual partners and any other individuals authorized to access the cloud by the Customer whose contact data will be processed.

- 2.6. Data processing shall take place exclusively in Germany, Austria and Switzerland.
- 2.7. Based on the service description specified in the CSA, it is the Customer's responsibility to carry out the correction, restriction, deletion, and disclosure of data themselves during the term of the agreement.. The rights of data subjects are to be exercised by the Customer. If the Customer requires the Contractor to be involved in the protection of data subjects' rights (particularly their right to information, rectification or erasure), then the Contractor must implement the relevant measures required immediately, following the Customer's instructions.

3. Technical and organizational measures

- 3.1. The Contractor must take appropriate technical and organizational measures as per Article 32 of the GDPR to ensure an appropriate level of data protection. The Contractor will structure their internal organization so as to ensure the implementation of and adherence to particular requirements from the Customer and the GDPR and/or national regulations.
- 3.2. The Contractor undertakes not to give any third party
 - a) direct, indirect, comprehensive or unrestricted access to data or
 - b) encryption keys used to secure data or the possibility of circumventing such encryption.
- 3.3. The document "Technical and Organizational Measures" outlines all technical and organizational measures that the Contractor must fulfill. By granting the order, the technical and organizational measures shall be deemed to have been checked and approved by the Customer. The most recent version of the "Technical and organizational measures" can be viewed online at the website listed in the CSA Information Sheet under "Link to Basis of the Contract".
- 3.4. The Contractor's data protection and data security concept is outlined in this document and in the other "Contractual Basis" documents specified in the CSA information sheet. The Contractor commits to evaluate and update this data protection and data security concept.
- 3.5. Evidence can also be provided by presenting attestations or reports by independent experts (e.g. auditors, inspections, accredited verifying authorities, data protection officers, IT security experts) or a suitable certificate.

4. Customer's instructions

- 4.1. The Customer is entitled to give written or oral instructions about the type, scope and method of data processing. The Customer shall confirm oral instructions in writing immediately. Only written instructions are binding for the Contractor.

If instructions from the Customer are not provided in the required form, the Contractor will inform the Customer of this.

- 4.2. The Customer will inform the Contractor of the individuals who are authorized to issue instructions or whose role is that of a contact person, specifying their name, organizational unit, function and telephone number. The Contractor will be informed in writing of any changes without delay.
- 4.3. Before the data processing commences, the Customer will make sure that the Contractor complies with the technical and organizational measures for data security. The Customer will inform the Contractor if there is any evidence of errors or irregularities when assessing the Customer's requirements or data protection regulations.
- 4.4. If the Contractor believes that an instruction from the Customer violates data protection regulations, he must inform the Customer immediately. If the Customer issues instructions that go beyond the contractually agreed scope of services, the associated cost and expenses must be borne by the Customer.

5. Duties of the Contractor; data confidentiality

- 5.1. The Contractor commits to processing and using the Customer's personal data solely for the services specified in the service description in the CSA, the Customer's instructions that are documented in writing and the current Agreement.
- 5.2. The Contractual Parties commit to preserving the confidentiality of each Contractual Party's critical business matters that are not common knowledge (trade secrets). The Contractor shall maintain data secrecy in accordance with the respective national regulations or the GDPR when storing the Customer's data.
- 5.3. The Contractor shall ensure that the employees involved in processing the Customer's personal data are bound to data secrecy when completing their tasks, in accordance with national regulations and/or the GDPR – even after this Agreement has expired – and that they have received instruction on the applicable data protection regulations.
- 5.4. The Contractor may pass on information to third persons or data subjects only if prior written consent is given by the Customer.
- 5.5. It is the Customer's responsibility to keep a record of all processing activities in accordance with Art. 30 (1) of the GDPR. The Contractor will support the Customer in this. The Contractor must keep their own record of processing activities in accordance with Art. 30 (2) of the GDPR and must provide this to the Customer upon request. The Contractor shall support the Customer in their responsibility with regard to any data protection impact assessment to be carried out and consultation with the supervisory authorities.
- 5.6. The Contractor shall inform the Customer without delay about control actions; investigations and measures of the supervisory authority under data protection law.

Should the Contractor be required to appear before a court or another government authority within the framework of a legal obligation or legal process and the Contractor is obligated to make user data stored by the Customer available for the court or the government authority, The Contractor shall proceed as follows:

- I. Governmental requests for information are thoroughly checked for their legality by qualified persons before they are complied with.

As long as the Contractor is not in violation of any laws, The Contractor shall contact the Customer as quickly as possible (electronically) in order to give the Customer the opportunity to take legal action to prevent disclosure of the data at the Customer's own expense.

The Contractor will only permit access after a positively completed check (cf. item i.) and will cooperate with the Customer to the extent legally possible in order to protect the Customer's data protection rights.

- II. The Contractor will only allow access to data covered by the request for information, insofar as this is possible using proportionate means. The Contractor must rely on the support of the Customer in order to determine which data is covered by the request for information and which is not, as the Contractor is not aware of the data stored in the Service Package.

5.7. The Contractor undertakes to regularly monitor compliance with the provisions of data protection law in their area of responsibility and to make any necessary adjustments to regulations and/or measures for proper commissioned processing.

5.8. The Contractor has a data protection team at their disposal that is dedicated to data protection issues ("Privacy Team"). The contact details of this Privacy Team are available at the website listed in the CSA Information Sheet under "Additional Helpful Links", "Privacy Website". The privacy team can be contacted at the email address provided in the CSA Information Sheet under "Possible Contacts", "Data Privacy"

If the GDPR and/or national regulations require, the Contractor will appoint a data protection officer. The contact data of this data protection officer are available at the website listed in the CSA Information Sheet under "Additional Helpful Links", "Privacy Website".

5.9. The Contractor has an obligation to provide the Customer with any information the Customer deems necessary to carry out comprehensive checks on the data processing on request and within an appropriate time frame.

5.10. All complaints or uncertainties relating to the Service Package can be made through the following channels:

- Via email: "Possible Contacts", "Data Privacy" pursuant to the CSA Information Sheet
- Via mail: Head Office of the Contractor pursuant to the CSA Information Sheet

All complaints should be addressed to the Contractor in writing. In order to prevent misuse by unauthorized persons, evidence of the identity of the complainant must be provided to the Contractor in a suitable form.

The Contractor designs its contracts in accordance with the high standards of the European Cloud Code of Conduct (EU Cloud CoC) and regularly submits a declaration of compliance with the latest valid version of the EU Cloud CoC. Complaints in this regard can also be submitted to the EU Cloud CoC Monitoring Body at the link <https://eucoc.cloud/en/public-register/complaints/>.

6. Sub-processors

- 6.1. In accordance with the following provisions and taking into account Section 2.6, the Contractor shall be entitled to engage sub-processors or to replace those already engaged.

The Contractor shall only engage those sub-processors who provide sufficient guarantees that appropriate technical and organizational measures will be implemented in such a way that the processing will be in compliance with the applicable data protection provisions and will ensure the protection of the rights of the data subject. The Contractor may satisfy themselves of compliance with the data protection provisions on site with timely notice.

For the purposes of this provision, subcontracting relationships are understood to be those services which relate directly to the provision of the main service. This does not include ancillary services which the Contractor uses, for example, telecommunication services, postal/transport services, or the disposal of data carriers.

This also does not include ancillary services that serve the security of processing (e.g., measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems). The Contractor shall also enter into appropriate and legally compliant contractual agreements and control measures for outsourced ancillary services to ensure data protection and data security of the Customer's data.

The Contractor shall notify the Customer without delay of any intended subcontracting or change of sub-processor. The Customer shall then be granted a 60-day first period to object. If no objection is raised within 60 days on objectively justified grounds against the subcontracting or the change of the sub-processor, it shall be deemed approved.

An objectively justified reason shall be deemed to exist in particular if there are indications, that the provision of the contractual services is endangered or impaired by the assignment, the cooperation with the sub-processor endangers the fulfillment of legal or contractual obligations of a contracting party, in particular of supervisory regulations.

In the event that sub-processors are engaged, they shall be contractually obligated with regard to the requirements for confidentiality, data protection and data security in accordance with this Agreement. The Contractor shall contractually impose on the sub-processor, mutatis mutandis, the same obligations that are specified in this Agreement or in other agreements between the Customer and the Contractor. The Contractor shall be obliged to provide the Customer with information on the main content of the Contract and the implementation of the data protection obligations by the sub-processors upon request.

The Contractor shall be responsible to the Customer for all actions and omissions of the sub-processors they employ.

The use of companies affiliated with the Contractor within the European Union and Switzerland as sub-processors shall be deemed to have been approved by the Customer in any case upon conclusion of this Agreement. Affiliated companies are companies in which Fabasoft AG, directly or indirectly, currently or in the future

- a) holds more than half of the voting rights; or
- b) can appoint more than half of the members of the management or administrative body or of the bodies appointed to represent them by law; or
- c) has the right to manage the company's business.

The Customer acknowledges the legitimate interest of the Contractor to transfer personal data for internal management purposes within the group of companies to which the Contractor belongs, including the processing of personal data.

- 6.2.** In the event that the Customer objects to the sub-contracting for objectively justified reasons, the Customer and the Contractor shall be entitled – in the absence of a mutually agreed solution – to extraordinary termination in accordance with the provisions of the CSA at the latest at the time of the planned change.

This extraordinary right of termination entitles the Customer and the Contractor to terminate the contractual relationship in question, taking into account the formalities pursuant to Section 4.5 of the CSA. If the Customer has selected a payment period that lasts longer than the contractual relationship once extraordinary termination occurs, the Customer shall be refunded the fees that have been overcharged, factored on a monthly basis.

The Customer also has a right to extraordinary termination if the Contractor arbitrarily uses a sub-processor without obtaining the prior written consent of the Customer or does so contrary to an objectively justifiable objection of the Customer, and an amicable resolution is not possible.

- 6.3.** The current list of sub-processors is available online at the “Link to the Basis of the Contract” according to the CSA Information Sheet. The sub-processors listed in the aforementioned list at the time of conclusion of this agreement shall be deemed to have been approved by the Customer.

7. Control rights of the Customer

- 7.1.** The Customer shall satisfy themselves of the technical and organizational measures of the Contractor prior to the commencement of data processing and thereafter on a regular basis and shall document the result.

For this purpose, the Customer may request corresponding information from the Contractor or personally satisfy themselves after timely notification during normal business hours without disrupting the operating process.

- 7.2.** The Contractor undertakes to provide the Customer, upon written request and within a reasonable period of time, with all information required for the performance of an inspection.
- 7.3.** An overview of certifications and audits is available in the CSA Information Sheet under “Additional Helpful Links”, “Overview of Certifications and Audits” at the website provided there.

To verify the data security measures and/or compliance with data security measures, the Customer can request, in writing, an audit by an independent authority or carry out such an audit themselves, provided the Customer can prove that they have the required expertise to carry out this audit. The term “audit” also includes penetration tests.

The Customer will present and justify the need for this audit to the Contractor in writing, within a period of at most 14 days from the request being made. The audit should be carried out without causing disruption to Contractor’s operation, insofar as is possible. The content, scope, procedure, selection of the auditing body, scheduling, and commissioning shall then be agreed between the Customer and the Contractor.

The Customer who requests the audit must bear the reasonable costs themselves (i.e. costs of the audit and Fabasoft’s expenses). If the Contractor also incurs additional staffing costs

beyond this, the Customer must settle these additional costs in accordance with the Contractor's standard hourly rates.

The Contractor can also present the Customer who requests the audit with the internal provisions on conducting an audit. The Customer must adhere to these provisions.

The Customer will present the Contractor with the audit documentation in the form of the entire audit report.

The Contractor can also comply with the Customer's request as a matter of priority by providing the Customer with a list of the current audit reports of audits previously carried out.

In any case, a corresponding non-disclosure agreement (NDA) must be signed by the Customer, the Contractor and the independent auditing authority before starting.

The summary of an audit report and the audit reports themselves should be treated as strictly confidential documents. Any form of transfer, distribution, or disclosure that has not been expressly approved in writing by the Contractor and, if provided for in the respective audit report, also by its auditor, is strictly prohibited.

If the Customer requires copies of the audit report from audits previously carried out on the Contractor for the purposes of assessment procedures, investigations or measures taken by the data protection supervisory authorities, then the Contractor will support the Customer – at their request – to fulfill their obligations to the supervisory authorities and transfer the required audit reports directly to the supervisory authorities.

- 7.4.** The Contractor is obliged to notify the Customer immediately in text form of any breach of data protection regulations in such a way that the Customer can fulfill their legal obligations. The same applies in the event of sufficient suspicion of suspected data protection violations or irregularities in the processing of personal data.

8. Data breach incident

- 8.1.** The Contractor is aware of the applicable data protection reporting and notification obligations vis-à-vis the supervisory authority and data subjects, in particular their time and content requirements.
- 8.2.** In all cases, the Contractor shall immediately notify the Customer if breaches of regulations for the protection of the Customer's data or of the stipulations made in the order have occurred by them or by the persons employed by them. This shall also include, in particular, if serious operational disruptions occur, if a breach of the data protection regulations is suspected or if other irregularities occur in the processing of the Customer's data.
- 8.3.** The Contractor shall take appropriate measures to secure the data and to mitigate any possible adverse consequences for the data subject. To the extent that the Customer is subject to reporting or notification obligations, the Contractor shall support the Customer in this respect.

9. Rights of the data subject

- 9.1.** The Contractor shall support the Customer in fulfilling their obligation to respond to requests to exercise the rights of the data subjects. Data subject rights may include, in particular:

- a) Duty to inform and right to access data;
 - b) Right to correction, deletion and data portability;
 - c) Right to object and right to not exclusively automated decision-making in individual cases.
- 9.2.** If data subjects contact the Contractor directly for the purpose of exercising their data subject rights, the Contractor shall forward this request to the Customer without delay.
- 9.3.** Likewise, any revocation of consent received by the Contractor from a data subject within the meaning of Art 7 (3) GDPR shall be forwarded to the Customer immediately.

10. Return of the data at the end of the contract

- 10.1.** The Contractor shall not have access to the Customer's user data. These personal data are in the exclusive power of disposal of the Customer. Therefore, the Customer shall immediately delete the data stored by themselves at the end of the order. Alternatively, the Customer may have the Contractor carry out the deletion. In this case, written instructions must be issued to the Contractor and access to the data must be granted, and the costs and expenses incurred by the Contractor in connection with the deletion must be borne by the Customer.
- 10.2.** The Customer shall determine the measures for the return and/or deletion of the stored data after termination of the order by contract or by instruction. The Customer shall also specify a time frame in which the return and/or deletion is to take place. Otherwise, the data shall be deleted or irretrievably returned by the Contractor no later than 6 months after termination of the contractual relationship. All costs in connection with the termination and/or return of the data shall be borne by the Customer.
- 10.3.** The data of the Customer, which may be useful, for example, for the proof of proper and order-compliant processing, may be stored by the Contractor's premises beyond the end of the contract, if justified, in accordance with data protection regulations.

11. Miscellaneous

- 11.1.** If the Customer's data is no longer safe or at risk at the Contractor's premises due to an attachment, execution or seizure or due to insolvency or composition proceedings or due to any other event or act of a third party, the Contractor shall notify the Customer immediately. The Contractor shall immediately inform all parties responsible in this context that the power over the data lies with the Customer.
- 11.2.** The Contractor and the Customer agree that amendments, additions and declarations relating to this agreement must be made in writing. The waiver of this written form requirement must also be made in writing. If amendments to this agreement are necessary due to changes in the legal basis, e.g. changes in the law or supreme court rulings, the amendment shall take effect on the respective date of its entry into force (see cover sheet, date).
- 11.3.** This Agreement shall be governed by the laws of the Contractor's place of business to the exclusion of any conflict of laws rules and of the UN Convention on Contracts for the International Sale of Goods. The place of jurisdiction shall be the locally competent court having jurisdiction at the Contractor's place of business.
- 11.4.** Should any provision of this Agreement be or become invalid or unenforceable, this shall not affect the validity of its remaining provisions. The contractual parties undertake to agree on a new, effective provision in place of the invalid provision which comes as close

as possible to the meaning and purpose of the invalid provision. This also applies to any omissions in the Agreement.

- 11.5.** For the purposes of this Agreement and Contractor's contact, Customer shall designate and keep current a contact in the mandatory field provided for that purpose in the Service Package. The Customer acknowledges that the Contractor shall direct all messages arising from and/or in connection with data security and data protection matters, in particular in accordance with item 8., exclusively to this contact set up by the Customer.