Data Processing Agreement

– the "**Contract**“ or "**Agreement**“ –

between

the customer specific in the quote

– the **“Client**" or **“Responsible Party**“ –

and

Zive GmbH
Große Bleichen 1-3
20354 Hamburg
Germany

– the "**Contractor**" or **“Processor**“ –

individually or together too **"Party”** and/or **“Parties**“

Version of September 25, 2025

1. Legal basis, subject matter, duration of the Contract

1.1. This agreement is based on the provisions of the EU General Data Protection Regulation (GDPR).

1.2. The subject of this Contract is the collection and processing of personal data by the Contractor on behalf of the Responsible Party on his behalf and according to his instructions in connection with the respective conditions of the cloud hosting services. The processing purpose is to provide and operate the software and to ensure its security in accordance with service description in Annex 1. The type and scope of processing, personal data and the categories of data subjects can also be found in Annex 1.

1.3. The duration of this Contract depends on the duration of the processing purpose in accordance with paragraph 2 of this section, unless otherwise stated in the following provisions. The right to termination without notice for good cause remains unaffected.

2. Rights and obligations of the Responsible Party

2.1. Within the framework of this Contract, the Client is responsible for compliance with the legal provisions of data protection laws, in particular for the legality of the data transfer to the Contractor and for safeguarding the rights of the data subjects.

2.2. The Contractor will only process personal data based on documented instructions from the Client - including the transfer of personal data to a third country or an international organization - unless he is required to do so by European Union or member state law to which the Contractor is subject and obliged. In such a case, the Contractor will inform the Client of these legal requirements before processing, unless the relevant law prohibits such communication due to important public interest. Changes to the object of processing and changes to the process must be agreed upon together and documented. If the Contractor is of the opinion that an instruction violates data protection regulations, he must inform the Client immediately. The Contractor is entitled to suspend the implementation of the relevant instructions until they are confirmed or changed by the Client. The Contractor may refuse to carry out an obviously illegal instruction.

2.3. The Contractor will only entrust sufficiently qualified and reliable staff with data processing. In particular, the Contractor will oblige the staff who can access the Client's personal data to maintain data secrecy (confidentiality) and inform them about the data protection obligations resulting from data processing and existing instructions or purpose limitations.

2.4. The Contractor appoints a Data Protection Officer (DPO), who will be announced in the Contractor's current and publicly available data privacy policy.

2.5. The Parties support each other promptly and comprehensively in examining possible violations and defending against claims from affected persons or third parties as well as against sanctions by supervisory authorities. The Contractor supports the client in particular in fulfilling its tasks in accordance with Articles 32 to 36 of the GDPR and in fulfilling its obligation to respond to requests to exercise the rights of data subjects listed in Chapter III of the GDPR.

2.6. Upon written request, the Contractor shall provide the Client at any time within a reasonable period of time with all available information and evidence that is necessary to assess whether the data processing is in accordance with the Contract. The Client makes sure before starting data processing and then regularly of the compliance with the regulations for the protection of personal data as agreed in this Contract, in particular of compliance with the agreed technical and organizational measures of the Contractor, and documents the results. For example, he can:

a. Obtain self-disclosure from the Contractor,

b. have a certificate from an expert or certificates presented to you, or

c. after announcing reasonably ahead of time during normal business hours and without disrupting any operational process, personally or through a knowledgeable third party, who must not be in a competitive relationship with the Contractor, convince you of compliance with the agreed regulations.

2.7. If there is any suspicion of violations of contractual obligations by the Contractor or the people employed by him to process orders or other violations of data protection regulations, the Contractor will immediately inform the Client in text form.

3. Technical and organizational measures

3.1. The Client and the Contractor will take appropriate technical and organizational measures (TOM) to secure the Client's data against misuse and loss, so that a level of appropriate protection for the relevant data protection regulations - in particular the GDPR - can be guaranteed.

3.2. The Contractor's TOMs as listed and described in Annex 2 are deemed suitable by the Parties for the purposes of this Agreement.

3.3. The TOMs are subject to technical progress and further development. In this respect, the Contractor is permitted to implement alternative measures. It must be ensured that the contractually agreed level of protection is not fallen short of. Significant changes must be agreed upon and documented.

4. Return and deletion

4.1. At the Client's request, the Contractor will return or delete all documents, data and data carriers provided to him, unless there is an obligation to store the personal data under European Union law or the law of the Federal Republic of Germany. This also applies to any test data. After the return request has been made, the parties will agree on further return modalities (e.g. format, deadline).

5. Sub-processors

5.1. The contractually agreed services are carried out with the involvement of the sub-processors listed in Annex 3. Within the framework of this Contract, the Contractor is authorized to establish further subcontract relationships for the provision of services.

5.2. The Contractor carefully selects sub-processors based on their suitability and reliability. The Contractor is obliged to bind the sub-processors in accordance with this Agreement. In particular, the Contractor ensures that the Controller can exercise his rights under this Agreement directly vis-à-vis the sub-processors, that the sub-processors provide sufficient guarantees that they are subject to the same data protection obligations as the Contractor and the TOMs of the sub-processors are carried out in such a way that they meet the requirements of this Agreement. The Processor must provide the Responsible Party with information about the data protection-related obligations of the sub-processors upon written request. If necessary, this also includes inspection of the relevant contract documents.

5.3. The Contractor will inform the Responsible Party by email of any intended change regarding the addition or replacement of sub-processors, giving the Responsible Party the opportunity to object to such changes on good cause within 14 days. The Contractor has an extraordinary right of termination if the Responsible Party objects to the involvement of the sub-processor without good cause.

5.4. Sub-processors of the sub-processors are also considered sub-processors. Orders given by the Processor to third parties to support the execution of this Agreement or the provision services, and that do not include any data processing services are not to be understood as subcontract relationships within the meaning of this regulation. In particular, additional services provided as telecommunications services, postal/transport services, maintenance and user services or the disposal of data media as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems, are not considered as subcontract relationships..

5.5. The transfer of personal data to countries outside the European Economic Area may only take place if the special requirements of Article 44 and following of the GDPR are met (e.g. by complying with the EU Data Privacy Framework or adopting standard contractual clauses approved by the European Commission in accordance with Article 46(2) of EU Regulation 2016/679 as amended on 4 June 2021.

6. Liability

6.1. The Client is responsible for the compensation of damages suffered by a data subject due to data processing that is impermissible or incorrect under the GDPR or other data protection regulations within the scope of the contractual relationship. If the Client is obliged to pay compensation, he reserves the right to recourse towards the Contractor if obligations from this Contract have been breached.

6.2. The Parties release themselves from liability if one Party proves that it is in no way responsible for the circumstances that caused the damage to an affected data subject.

7. Miscellaneous

7.1. This data processing agreement supersedes all previously agreed data processing agreements between the Parties related to the services.

7.2. Should individual provisions of this agreement prove to be invalid or unenforceable in whole or in part, or become invalid or unenforceable after conclusion of the Contract, the remaining contractual provisions and the effectiveness of the Contract as a whole remain unaffected. The invalid or unenforceable provision should be replaced by an effective and enforceable provision that comes closest to the meaning and purpose of the invalid provision or what the Parties intended.

7.3. German law applies, including European law such as the GDPR. Place of jurisdiction is Hamburg, Germany.

7.4. Changes and additions to this agreement and all of its components require a written agreement.

Details on the data processing of the Zive software

Description of services

Zive is a modern platform for AI and knowledge management in companies. The application's goal is to provide the customer's employees with a unified and secure AI work environment.

Further information on the type and scope of the software can be found in the offer and service descriptions.

Details about the processing of data

Description of the processing activity

Essentially the following tasks are carried out by the Contractor:

- Provision of software that serves internal knowledge management.
- Hosting of the client's data on an IT infrastructure provided by the Contractor and his sub-processors.

Categories of those affected, types of data, forms of access

a. Categories of data subjects

Basically, the software is used for internal knowledge management. If the Customer (Responsible Party) intends to process personal data from other categories in the software, this would have to be indicated below by the Responsible Party.

- [x] Employees
- [x] Customers
- [x] Suppliers
- [ ] Commercial Agents
- [ ] Interested Parties
- [ ] Contact persons for the above categories

b. Affected personal data

To use the software, users only need to provide their name and email address. In addition, the software accesses employees' public data. If the Customer (Responsible Party) wants to use other types of data in the software, this must be indicated by the Responsible Party using additional crosses below.

- ☑ Last name, First name
- ☑ Profile photo
- ☐ Address
- ☐ Place of birth
- ☐ Marital status
- ☑ Contact details (e.g. telephone, email)
- ☐ Address
- ☐ Signature
- ☑ Inventory data (e.g. billing address, contract number)
- ☐ Traffic data (e.g. connection ID, location data, start/end of a telephone connection)
- ☑ Contract master data
- ☐ HR master data
- ☑ Communication data
- ☐ Billing data
- ☑ Customer history
- ☐ Nationality
- ☑ Profession
- ☐ Bank account
- ☐ Miscellaneous:

c. Sensitive data / special categories of data in accordance with Section 9 GDPR

No sensitive data is required to use the software. If the Responsible Party wants to process sensitive data in the software, this must be supplemented by the Responsible Party.

d. Access to personal data

The Processor provides services in the area of hosting, but also maintenance, remote maintenance or IT error analysis. The possibility of the Processor gaining access to data cannot be ruled out. The following extended obligations apply:

- The Processor will make as little use of the access rights granted to him - including in terms of time - as is necessary for the proper execution of the commissioned maintenance and testing work.
- The Processor will send a separate notification (by email/in writing) about upcoming testing and maintenance work to the Responsible Party before the work begins.
- At the request of the Responsible Party, the Processor informs what work will be carried out and when.

Technical and organizational measures to ensure the security of data processing

Zive GmbH guarantees that it has taken the following technical and organizational measures:

A. Pseudonymization measures

Measures that reduce the direct personal reference during processing in such a way that an assignment to a specifically affected person is only possible with additional information. The additional information must be stored separately from the pseudonym using appropriate technical and organizational measures.

- Pseudonymization is used wherever possible as long as it does not restrict the performance of the main contract.
- Selection of a suitable pseudonymization process according to latest technological standards.

B. Encryption measures

Measures or processes in which a clearly readable text/information is converted into an illegible, i.e. not easily interpretable, character string (ciphertext) using an encryption process (cryptosystem).

- All data transferred from the Responsible Party to the Processor, as well as all data transferred between the Processor's systems during processing, is encrypted using TLS 1.2 or better.
- All data stored on disks is encrypted using AES 256 or better.

C. Measures to ensure confidentiality

C1. Physical access control

Measures that physically prevent unauthorized persons from accessing IT systems and data processing systems used to process personal data, as well as confidential files and data storage media.

- Does not apply because the Processor does not operate its own IT systems or data processing systems that process personal data.
- Guidelines for mobile working / home office.
- The access control measures of the cloud providers used (subcontractors) also apply, in particular Microsoft Azure EU.
- In addition, the following access control measures apply to prevent unauthorized access to the cloud provider's systems.

C2. Logical access control

Measures to prevent unauthorized persons from processing or using data protected by data protection law.

- Password policy (including stipulations regarding the use of special characters, minimum length, regular change of password, prohibition of sharing)
- Authentication only with 2FA or biometric passkeys
- Guidelines for mobile working / home office
- Automatic screen lock
- Logging of authentication attempts and account lockout after multiple unsuccessful attempts
- Exclusive storage of server and client secrets in specially designed and secured key vaults ("Key Vault")
- Use of individual user accounts
- Limiting the number of eligible employees
- Regular review of roles and access lists
- Prohibition of the use of private data carriers
- Encryption of all data carriers ("at rest")
- Device tracking and remote locking

C3. Data access control

Measures that ensure that those authorized to use the data processing procedures can only access the personal data subject to their access authorization, so that data cannot be read, copied, changed or removed without authorization during processing, use and storage.

- Authorized persons can only access data that is set up in the individual authorization profile
- The scope of authorizations is limited to the minimum necessary to fulfill the respective task or function (logical, temporal, ...)
- Limiting the number of eligible employees
- Regular review of roles and access lists
- Use of user-related and individualized login information, especially use of individual user accounts
- Password policy, especially no sharing of passwords
- Prohibition of the use of private data carriers
- Encryption of all data carriers ("at rest")
- Data access logging:
    - All read, input, change and delete transactions are logged (user ID, transaction details) and archived in an audit-proof manner for at least 6 months
    - Random evaluations are carried out regularly to detect misuse

C4. Separation requirement

Measures to ensure that data collected for different purposes are processed separately from other data and systems in such a way that unplanned use of this data for other purposes is excluded.

- User profiles / separation of user accounts
- Different access permissions
- Logically separate storage on the same systems / client separation
- Separation of processing systems
- Separation of productive and test systems
- No productive data in test systems

C5. Further measures

- Confidentiality agreements with internal and external employees
- Confidentiality agreements with external service providers
- Security agreements with external service providers
- Consideration of the principles of data protection through technology and the data protection-friendly basic settings (Privacy by Design, Privacy by Default)
- Limitation of permissible personnel to those who are verifiably responsible (locally, professionally), professionally qualified, reliable (if necessary, security checked) and formally approved and who do not have any conflicts of interest when carrying out their duties

D. Measures to ensure integrity

D1. Data integrity

Measures to ensure that stored personal data is not damaged by system malfunction.

- Encryption of all data “in transit” and “at rest” (see above)
- Logically separate storage on the same systems / client separation
- Separation of processing systems
- Separation of productive and test systems
- No production/live data in test systems
- Fully automated release processes via version control system
- Automated testing procedures
- Application of the principle of least privilege
- Logging (e.g. server logs, network logs)

D2. Transmission control

Measures to ensure that it can be verified and determined to which bodies personal data have been or can be transmitted or made available using data transfer facilities.

- Container-based server systems (virtually sealed-off networks)
- Measures to prevent attacks (e.g. virus scanner, firewall)
- Encryption of data transmission, especially when transmitted via public networks (e.g. SSL, TLS)
- Encryption of data carriers (“at rest”)
- Use of individual user accounts
- Limiting the number of eligible employees
- Regular review of roles and access lists

- Logging (e.g. server logs, network logs)

D3. Transport control

Measures to ensure that the confidentiality and integrity of the data is protected when transmitting personal data and transporting data carriers.

- Container-based server systems (virtually sealed off networks, including L2TP, IPSec)
- Encryption of data transmission, especially when transmitted via public networks (e.g. SSL, TLS)
- Encryption of data carriers (“at rest”)
- Measures to prevent attacks (e.g. virus scanner, firewall)
- Logging (e.g. server logs, network logs, deletion logs)

D4. Input control

Measures that ensure that it can be subsequently checked and determined whether and by whom personal data has been entered, changed or removed in computer systems.

- Regular review of roles and access lists
- Audit trailing of all configuration and data changes (e.g. “Azure Activity Logs”)
- Logging (e.g. server logs, request logs)

E. Measures to ensure availability and resilience

E1. Availability control

Measures to ensure that personal data is protected against accidental destruction or loss.

- Measures to prevent attacks (e.g. virus scanner, firewall)
- Container-based server systems (virtually sealed off networks)
- Automatic monitoring with numerous notification channels
- Creation of regular backups
- Regular penetration tests
- Further, the availability control measures of the cloud providers used (subcontractors), in particular Microsoft Azure EU, also apply.

E2. Rapid recoverability

Measures to ensure the ability to quickly restore the availability and access to personal data in the event of a physical or technical incident.

- Use of “Infrastructure as Code” and separation of application and data systems
- Geo-redundant storage
- Automated recovery procedure
- On-call service 24/7

E3. Reliability

Measures to ensure that all functions of the system are available and any malfunctions that occur are reported.

- Automatic load balancing and automatic system scaling under load
- Exclusive collaboration with proven cloud providers, especially Microsoft Azure EU, who use suitable backups, geo-redundancy and failover techniques
- Automatic monitoring with numerous notification channels
- Conducting penetration tests regularly
- Use of “Infrastructure as Code” and separation of application and data systems
- On-call service 24/7

F. Measures for regular evaluation of the security of data processing

F1. Verification procedure

Measures that ensure data protection-compliant and secure processing.

- Regular checking of the hardware and software inventory according to an inventory and annual updating of the inventory
- Regular checking of data processing systems and processing activities for security gaps that may arise due to new technical developments or changed processing practices
- Regular version control of standard software (intensity of control depends on the software used, but testing should take place at least once a year)
- Regular audits with the data protection officer

F2. Order control

Measures to ensure that personal data processed on behalf of the customer can only be processed in accordance with the instructions of the client.

- Established criteria for selecting contractors (references, certifications, seals of quality)
- Legally compliant drafting of contracts for the data processing of personal data with subcontractors with appropriate regulation of control mechanisms
- Contractual agreement with subcontractors to oblige their own and external employees to maintain data secrecy
- Obtaining self-information from service providers regarding their measures to implement data protection requirements
- Limiting the number of authorized employees/user accounts

F3. Incident-Response-Management

In the event of a breach of the protection of personal data, the person responsible is obliged (Article 33 GDPR) to report this to the competent supervisory authority in accordance with Article 55 immediately and, if possible, within 72 hours of becoming aware of the breach, unless the breach the protection of personal data is unlikely to result in a risk to the rights and freedoms of natural persons. If the report is not made to the supervisory authority within 72 hours, it must be accompanied by a justification for the delay.

Measures in the event of a data protection incident:

- Verification of suspected cases
- Description of the process of what happens in the event of a data breach
- Description of responsibilities
- Description of the technical process for eliminating a data breach

F4. Further measures

- Privacy-friendly presets
    - Minimizing the amount of data collected
    - Reducing the amount of data processing
    - Reduction of storage periods
- Written designation of the data protection officer (DPO)
- The DPO is involved in the data protection impact assessment
- Training of employees in data protection law, including the obligation of employees to maintain confidentiality when handling personal data
- Legal obligation of employees to comply with internal security and data protection guidelines

Information about sub-processors for the Zive software

The following sub-processors may be used under these agreements:

Name	Address	Services	Data process location	International data transfer	Data processing basis (for non-EU)
Microsoft Ireland Operations, Ltd.	One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland	Cloud compute and AI models	EU	No	Not applicable
Intercom, Inc.	55 2nd Street, 4th Fl., San Francisco, CA 94105, USA	Service and help desk	EU	No	Not applicable
Heureka Labs UG	Haidkoppelweg 27b 21465 Reinbek Germany	AI services	EU	No	Not applicable
Mistral AI*	15 Rue des Halles 75001 Paris, France	AI services	EU	No	Not applicable
Tavily Inc.*	AlphaAI Technologies Inc., dba Tavily 051 Frederick Douglass 5B NY 10026, USA	Web search	USA	Yes	Standard Contractual Clauses (SCCs)

Annex 3

Name	Address	Services	Data process location	International data transfer	Data processing basis (for non-EU)
Google LLC*	1600 Amphitheatre Parkway Mountain View CA 94043, USA	AI models	EU, USA	Yes	EU-U.S. Data Privacy Framework (DPF)
Amazon Web Services Inc.*	410 Terry Avenue North, Seattle, WA 98109-5210, USA	AI models	EU, USA	Yes	Standard Contractual Clauses (SCCs)
Anthropic PBC*	548 Market St, San Francisco, USA	AI models	EU, USA	Yes	Standard Contractual Clauses (SCCs)

* Only applicable when switched on manually by the client in the platform administration.