Data Processing Agreement

This Data Processing Agreement regulates data processing on behalf of the customer by **ATLAS.ti Scientific Software Development GmbH** as a data processor. It becomes part of the respective agreement by reference in the Terms of Use.

Preamble

The Contractor processes personal data on behalf and on instruction of the Client within the meaning of Article 4 No. 8 and Article 28 of Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). This Data Processing Agreement regulates the rights and obligations of the parties in connection with the processing of personal data.

1. Definitions

1.1 Pursuant to Art. 4 para. 7 GDPR, "Controller" is the body which alone or jointly with other controllers decides on the purposes and means of processing personal data.

1.2 According to Art. 4 para. 8 GDPR, "Processor" is a natural or legal person, authority, institution or other body that processes personal data on behalf of the Controller.

1.3 According to Art. 4 para. 1 DPA, "Personal Data" shall mean any information relating to an identified or identifiable natural person (hereinafter referred to as "data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, a location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.4 "Particularly Sensitive Personal Data" are personal data pursuant to Art. 9 GDPR, from which the racial or ethnic origin, political opinions, religious or ideological convictions or trade union membership of the persons concerned can be deduced, personal data pursuant to Art. 10 GDPR on criminal convictions and offences or related security measures as well as genetic data in accordance with Art. 4 Para. 13 GDPR, biometric data in accordance with Art. 4 Para. 14 GDPR, health data in accordance with Art. 4 Para. 15 GDPR and data concerning the sexual life or sexual orientation of a natural person.

1.5 Pursuant to Art. 4, para. 2 GDPR, "Processing" is defined as any operation or set of operations, performed with or without the aid of automated procedures, concerning personal data, such as collection, recording, organization, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction.

1.6 According to Art. 4 para. 21 GDPR, "Supervisory Authority" is an independent state body established by a Member State according to Art. 51 GDPR.

2. Subject Matter

2.1 Contractor shall provide services for Client in the area of "provision of software" on the basis of the Main Contract concluded between the parties. Within the scope of the Main Contract, the Contractor shall be granted access to personal data and shall process such data exclusively on behalf of and in accordance with the instructions of the Client. The object of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects are set out in Annex 1 to this Data Processing Agreement. It is the responsibility of the Client to assess the permissibility of the data processing.

2.2 The parties conclude this Data Processing Agreement in order to concretize the mutual data protection rights and obligations. In case of doubt, the provisions of this Agreement shall take precedence over the provisions of the Main Contract.

2.3 The provisions of this Data Processing Agreement shall apply to all activities related to the Main Contract in which the Contractor and its employees or agents commissioned by the Contractor come into contact with personal data originating from or collected for the Client.

2.4 This Data Processing Agreement shall commence upon signature; the term of this Data Processing Agreement shall be based on the term of the Main Contract, unless the following provisions impose obligations or rights of termination that go beyond this.

3. Instruction

3.1 The Contractor may only collect, process or use data within the framework of the Main Contract and in accordance with the instructions of the Client; this applies in particular with regard to the transfer of personal data to a third country or to an international organization. If the law of the European Union or of the Member States to which the Contractor is subject requires further processing, the Contractor shall notify the Client of these legal requirements prior to processing.

3.2 The Client's instructions are initially set out in this contract and may subsequently be amended, supplemented or replaced by individual instructions in writing or in text form (individual instructions). The Client is entitled to issue corresponding instructions at any time. This includes instructions regarding the correction, deletion and blocking of data. Oral instructions must be confirmed immediately in writing or in text form.

3.3 All instructions issued must be documented by both the Client and the Contractor. Instructions that go beyond the performance agreed in the Main Contract will be treated as a request for a change in performance.

3.4 If the Contractor is of the opinion that an instruction of the Client violates data protection regulations, the Contractor must inform the Client of this immediately. The Contractor is entitled to suspend the execution of the instruction in question until it is confirmed or amended by the Client. Contractor may refuse to carry out an obviously illegal instruction.

4. Data Categories, Data Subjects

In the course of the execution of the Main Contract, the Contractor shall be granted access to the personal data specified in **Appendix 1.** The data subjects affected by the data processing are also defined in **Appendix 1.**

5. Obligations of the Contractor

5.1 The Contractor is obliged to observe the legal provisions on data protection and not to pass on information obtained from the Client's sphere to third parties or to grant third parties access to such information. Documents and data must be secured against unauthorized access, taking into account the state of the art.

5.2 Within its area of responsibility, the Contractor shall design the internal organization in such a way that it meets the special requirements of data protection. The Contractor shall take all necessary technical and organizational measures for the appropriate protection of the Client's data in accordance with Art. 32 GDPR, in particular at least the measures listed in **Appendix 2**. The Contractor reserves the right to change the security measures taken, whereby he shall ensure that the contractually agreed level of protection is not compromised.

5.3 The persons employed by the Contractor in data processing are prohibited from collecting, processing or using personal data without authorization. The Contractor shall impose a corresponding obligation on all persons entrusted by him with the processing and fulfilment of this contract (hereinafter referred to as employees) (obligation of confidentiality, Art. 28 para. 3 lit. b GDPR) and shall ensure compliance with this obligation with due care. These obligations must be formulated in such a way that they remain in force after the termination of this contract or the employment relationship between the employee and the Contractor. On request, the Client must be provided with suitable evidence of the obligations in a suitable manner.

6. Information Duties of the Contractor

6.1 In the event of malfunctions, suspicion of data protection violations or breaches of contractual obligations on the part of the Contractor, suspicion of security-related incidents or other irregularities in the processing of personal data by the Contractor, persons employed by the Contractor within the scope of the order or by third parties, the Contractor shall inform the Client immediately in writing or in text form. The same applies to audits of the Contractor by a data protection supervisory authority. The notification of a violation of the protection of personal data shall contain at least the following information:

a) a description of the nature of the breach of personal data protection, including, as far as possible, the categories and the number of data subjects, the categories and the number of personal data records concerned

b) a description of the measures taken or proposed by the Contractor to remedy the breach and, where appropriate, measures to mitigate its possible adverse effects

6.2 The Contractor shall immediately take the necessary measures to secure the data and to mitigate possible adverse consequences of the affected parties, shall inform the Client thereof and request further instructions.

6.3 Furthermore, the Contractor is obliged to provide the Client with information at any time, insofar as the Client's data is affected by a violation pursuant to Clause 6.1.

6.4 If the data of the Client are endangered at the Contractor by seizure or confiscation, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor has to inform the Client immediately, unless this is prohibited by court or official order. In this context, the Contractor shall immediately inform all competent authorities that the authority to decide on the data lies exclusively with the Client as the Controller.

6.5 The Contractor shall inform the Client without delay of any significant change in the security measures pursuant to Clause 5.2.

6.6 The Client must be informed immediately of any change in the person of the data protection officer/contact person for data protection.

6.7 The Contractor and, if applicable, his representative shall keep a register of processing activities carried out on behalf of the Client, which shall contain all the information required by Art. 30 para. 2 GDPR. The list shall be made available to the Client on request.

6.8 The Contractor shall cooperate to an appropriate extent in the preparation of the list of procedures by the Client. The Contractor must provide the Client with the necessary information in a suitable manner.

7. Audit Rights of the Client

7.1 The Client has the right to check at any time to the extent necessary that the Contractor complies with the statutory provisions on data protection and/or the contractual provisions agreed between the parties and/or the Contractor's compliance with the Client's instructions. The Contractor is entitled to prove the compliance with the obligations laid down in this Data Processing Agreement by suitable means, including self-audits, certificates, etc.

7.2 The Contractor is obliged to provide information to the Client to the extent that this is necessary to carry out the inspection as defined in paragraph 1 above.

7.3 If necessary in individual cases, the Client may demand an inspection of the data processed by the Contractor for the Client and of the data processing systems and programs used.

7.4 After prior notification and with a reasonable period of notice, the Client may carry out the inspection within the meaning of paragraph 1 at the Contractor's premises during normal business hours. In doing so, the Client shall ensure that the inspections are only carried out to the extent necessary to avoid disproportionately disturbing the Contractor's business operations. The parties assume that an inspection is required at most once a year. Further inspections shall be justified by the Client, stating the reason. In the case of on-site inspections, the Client shall reimburse the Contractor for the expenses incurred, including personnel costs, for the supervision and accompaniment of the inspectors on site to a reasonable extent. The bases for the calculation of costs will be communicated to the client by the Contractor before the inspection is carried out. The Contractor may make the controls dependent on prior notification with an appropriate lead time and on the signing of a confidentiality agreement. If the inspector commissioned by the Client is in a competitive relationship with the Contractor, the Contractor has a right of objection.

7.5 At Contractor's option, proof of compliance with the technical and organizational measures may also be furnished, instead of an on-site inspection, by the submission of a suitable, up-to-date audit certificate, reports or report extracts from independent bodies (e.g. auditors, revision, data protection officer, IT security department, data protection auditors or quality auditors) or suitable certification, if the audit report enables the Client to satisfy itself in a reasonable manner that the technical and organizational measures in accordance with **Appendix 2** to this Data Processing Agreement are being complied with. If the client has reasonable doubts about the suitability of the test document within the meaning of sentence 1, an on-site inspection can be carried out by the Client. The Client is aware that an on-site inspection in data centers is not possible or only possible in justified exceptional cases.

7.6 In the event of measures taken by the supervisory authority against the Client within the meaning of Art. 58 GDPR, in particular with regard to duties of information and control, the Contractor shall be obliged to provide the Client with the necessary information and to enable the respective competent supervisory authority to carry out an on-site inspection. The Client shall be informed by the Contractor about corresponding planned measures.

7.7 The Contractor shall prove to the Client the obligation of the employees according to Clause 5.3 upon request.

8. Use of Subcontractors

8.1 The Contractor is entitled to use subcontractors for the processing of Client’s data. The Contractor must carefully select the subcontractors and check before the order is placed that they can comply with the agreements made between the Client and the Contractor. In particular, the Contractor shall check in advance and regularly during the term of the contract that the subcontractor has taken the technical and organizational measures required under Art. 32 GDPR for the protection of personal data

8.2 The Client agrees that the Contractor use further subcontractors or replace subcontractors if necessary. Contractor shall inform Client of such changes within a reasonable period of time in advance in electronic form. The Client may object to the change for good cause within a reasonable period determined by Contractor at its reasonable discretion. If no objection is made within this period, the consent to the change shall be deemed to have been given.

8.3 The Contractor is obliged to obtain confirmation from the subcontractor that the latter has designated a data protection officer in accordance with Art. 37 GDPR, provided that the subcontractor is legally obliged to designate a data protection officer.

8.4 Contractor shall ensure that the provisions agreed in this Data Processing Agreement and any supplementary instructions of the Client shall also apply to the subcontractor.

8.5 The Contractor is in particular obliged to ensure by contractual provisions that the audit rights of the Client and supervisory authorities also apply to the subcontractor and that corresponding control rights are agreed by the

Client and supervisory authorities. In addition, it shall be stipulated in the contract that the subcontractor shall tolerate these control measures and any on-the-spot checks.

8.6 Subcontracting relationships within the meaning of paragraphs 1 to 5 shall not be deemed to be services which the Contractor uses from third parties as a purely ancillary service in order to carry out the business activity. These include, for example, cleaning services, pure telecommunications services without any specific reference to services which the Contractor provides for the Client, postal and courier services, transport services, security services. The Contractor is nevertheless obliged to ensure, also in the case of ancillary services provided by third parties, that appropriate precautions and technical and organizational measures have been taken to ensure the protection of personal data. The maintenance and servicing of IT systems or applications constitutes a subcontracting relationship and data processing on instruction within the meaning of Art. 28 GDPR requiring approval if the maintenance and testing concerns such IT systems which are also used in connection with the provision of services for the Client and if personal data processed on behalf of the Client can be accessed during maintenance.

9. Data Subject Rights

9.1 The Client is solely responsible for safeguarding the rights of the data subjects. The Contractor supports the Client as far as possible with suitable technical and organizational measures in the fulfillment of the Client's obligations according to Art. 12 - 22 as well as 32 and 36 GDPR.

9.2 If a data subject asserts rights, such as the right to access/information, correction or deletion of his/her data, directly against the Contractor, the Contractor does not react independently, but refers the data subject to the Client immediately and waits for the Client's instructions.

10. Confidentiality Obligations

10.1 Both parties undertake to treat all information received in connection with the execution of this Data Processing Agreement as confidential for an unlimited period of time and to use it only for the execution of this Data Processing Agreement and/or the Main Contract. Neither party shall be entitled to use this information in whole or in part for purposes other than those just mentioned or to make this information available to third parties.

10.2 The above obligation shall not apply to information which one of the parties has demonstrably obtained from third parties without being obliged to maintain secrecy or which is publicly known.

11. Termination

After termination of the Main Contract or at any time at the request of the Client, the Contractor shall return to the Client all documents, data and data carriers provided to the Contractor or - at the request of the Client, unless there is an obligation to store personal data under Union law or the law of the Federal Republic of Germany - delete them. The deletion must be documented in a suitable manner and proof must be provided upon request.

12. Final Provisions

12.1 The parties agree that the defence of the right of retention by the Contractor (according to § 273 BGB) with regard to the data to be processed and the associated data carriers is excluded.

12.2 Changes and amendments to this Data Processing Agreement and all of its components - including any assurances given by the Contractor - require a written agreement, which may also be in electronic format (text form), and the express indication that this is a change or amendment to this Data Processing Agreement. This also applies to the waiver of this formal requirement.

12.3 Should individual provisions of this agreement be or become invalid or unenforceable in whole or in part, the validity of the remaining provisions shall not be affected.

12.4 This agreement is subject to German law.

Attachments:
Appendix 1: Description of the Processing
Appendix 2: Technical and Organizational Measures

Appendix 1: Description of the Processing

1. Scope and Purpose of the Processing

The Client's order to the Contractor includes the following work and/or services:

Provision of the Contractor's data analysis platform as SaaS

2. Type(s) of Personal Data

The following types of data are regularly subject to the data processing:

Data which the Client analyzes or processes using the Contractor's data analysis platform and the nature of which is determined by the Client at his own discretion and which may, for example, particularly include data on entities and projects of the Client, test persons, patients and other participants and affected persons within the framework of scientific studies and research projects.

3. Categories of Data Subjects

Data subjects affected by the data processing:

Categories of data which the Client analyzes or processes using the Contractor's data analysis platform and whose categories the Client determines at its own discretion and which may include, for example, the following categories of data: First name and surname, contact data, medical data, genetic data, biometric data, other special categories of personal data, data on living habits and other circumstances, information from interviews, customer feedback and behavioral data.

Appendix 2: Technical and Organizational Measures

1. Confidentiality (Article 32 (1) lit. b) GDPR)

a. Physical Access Control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used:

- Locking system with code lock
- Security locks
- Key control (key issuance etc.)
- Logging of visitors
- Careful selection of security personnel
- Careful selection of cleaning personnel
- Manual locking system

b. System Access Control

Measures that are suitable to prevent data processing systems from being used by unauthorized persons:

- Assignment of user rights
- Password assignment
- Authentication with username / password
- Use of anti-virus software
- Use of a software firewall

c. Data Access Control

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

- Administration of rights by system administrator
- Number of administrators reduced to the "bare minimum
- Logging of accesses to applications, in particular when entering, changing and deleting data
- proper destruction of data media (DIN 32757)
- Use of document shredders or service providers
- Logging of the destruction

d. Separation Control

Measures to ensure that data collected for different purposes can be processed separately:

- Logically strictly separated storage of data in different customer systems
- Encryption of data records that are processed for the same purpose
- Providing records with purpose attributes/data fields
- Separation of production and test system

2. Integrity (Art. 32 (1) lit. b) GDPR)

a. Transfer Control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transmission or during their transport or storage on data carriers, and that it is possible to check and establish to which bodies personal data are to be transmitted by data transmission equipment:

- A transfer of personal data, which is carried out on behalf of customers, may only take place to the extent agreed with the customer or to the extent necessary to provide the contractual services for the customer.
- All ATLAS.ti employees working on a customer project are instructed on the permissible use of data and the modalities of data transfer.
- As far as possible, data will be transmitted to recipients in encrypted form.
- ATLAS.ti employees are prohibited from using private data storage media in connection with customer projects.

b. Input Control

Measures to ensure that it can be subsequently checked and established whether and by whom personal data have been entered, modified or removed from data processing systems:

- Logging of data entry, modification and deletion
- Traceability of input, modification and deletion of data through individual user names (not user groups)

3. Availability and Resilience (Art. 32 (1) lit. b) GDPR)

a. Availability Control

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

- Uninterruptible Power Supply (UPS)
- Equipment for monitoring temperature and humidity in server rooms
- Fire and smoke detection systems
- Creation of a backup & recovery concept
- Creating an emergency plan
- Server rooms not under sanitary facilities
- Air conditioning in server rooms
- Protective socket strips in server rooms
- Fire extinguishing equipment in server rooms

b. Recoverability (Art. 32 (1) lit. c) GDPR)

Measures to ensure that personal data can be restored immediately in case of loss or disruption:

- Regular backups
- Testing data recovery

4. Procedures for Regular Review, Assessment and Evaluation (Art. 32 (1) lit. d) GDPR; Art. 25 (1) GDPR)

a. Data Protection and Information Security Management

At ATLAS.ti, a data protection management system is implemented. There is a guideline on data protection and data security and guidelines to ensure that the goals of the guideline are implemented. All guidelines are regularly evaluated and adjusted with regard to their effectiveness.

A Data Protection and Information Security Team has been set up to plan, implement, evaluate and make adjustments to data protection and data security measures.

A data protection officer has been appointed.

All employees receive regular training in data protection and information security.

b. Incident Response Management

All employees are instructed and trained to ensure that data privacy incidents are recognized by all employees and reported to the Data Protection and Information Security Team without delay. The Data Protection and Information Security Team will investigate the incident immediately. As far as data are concerned that are processed on behalf of clients, it is ensured that they are informed immediately about the nature and extent of the incident.

c. Privacy by Design and by Default (Art. 25 (2) GDPR)

At ATLAS.ti, we make sure that the principle of necessity and data minimization is taken into account right from the software development stage.

d. Order Control

Measures to ensure that personal data processed by order can only be processed according to the instructions of the client:

- Careful selection of subcontractors (especially with regard to information security)
- Regular control of the subcontractors