Data Processing Terms of Agreement

According to Art. 28 (3) General Data Protection Regulation (GDPR)

1. Subject-Matter and Duration of the Processing

1.1. This Data Processing Agreement (the **"Agreement"**) sets out the respective privacy and data protection rights and obligations of the parties in relation to the provision of services in accordance with the Description of Service, Terms of Services and General Terms and Conditions (hereinafter referred to as the "**Main Contract**"). This Agreement applies to the extent that IT-Co and/or our Partners(s) (hereinafter referred to as the "**Processor"**) processes personal data on behalf of the Customer as controller (hereinafter referred to as the client "Customer"), together referred to as the **"Parties"**. This includes all activities that the Processor performs to fulfil the Main Contract and that represent a data processing activity on behalf of the controller. This Agreement shall apply to any instructions from the Controller, regardless of whether such order or instruction explicitly refers to this Agreement.

1.2. Under this Agreement, the Parties agree that the terms "controller", "data subject", "personal data", "processing", "processor" and "third party/ies" shall have the meaning assigned to them in the Data Protection Legislation.

1.3. The duration of the processing corresponds to the term agreed in the Main Contract.

1.3.1 In this Agreement, the following definitions apply:

1.3.2 Data Protection Legislation means:

(a) to the extent UK GDPR applies, the law of the United Kingdom or of a part of the United Kingdom which relates to the protection of personal data.

(b) the extent the EU GDPR applies, the law of the European Union or

Data Processing Terms of Agreement

any member state of the European Union to which the Customer or Processor is subject, which relates to the protection of personal data.

1.3.3 EU GDPR means: the General Data Protection Regulations (EU) 2016/679).

1.3.4 UK GDPR: has the meaning given to it in section 3 (10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

2. Nature and Purpose of the Processing

2.1. The nature of the processing includes all types of processing required to fulfil the Main Contract with the Customer.

2.2. Purposes of processing are all purposes required to provide the contracted services in terms of hosting and IT support.

3. Type of Personal Data and Categories of Data Subjects

3.1. The type of processed data is determined by the Customer by the product selection, the configuration, the use of the services, and the transmission of data, in accordance with the Description of Service.

3.2. The categories of data subjects are determined by the Customer via product selection, configuration, the use of the services, and the transmission of data, in accordance with the Description of Service.

4. Responsibility and Processing on Documented Instructions

4.1. The Customer is responsible for complying with the legal requirements of the Data Protection Legislation, in particular, the legality of the transfer of data to the Processor and the legality of data processing under this Agreement. This also applies to the purposes and means of processing set out in this Agreement.

Data Processing Terms of Agreement

4.2 The instructions are initially determined by the Main Contract and can then be changed by the Customer in writing or in an electronic format (text form) by individual instructions (individual instruction). Verbal instructions must be confirmed immediately in writing or in text form. The instructions must be documented by the Customer and kept for at least the duration of the contractual relationship. In the event of proposed changes, the Processor shall inform the Customer of the effects that this will have on the agreed services, in particular, the possibility of providing services, deadlines, and remuneration. If the implementation of the instruction is not reasonable to the Processor, the Processor is entitled to terminate the processing. The Processor has the right to reject any instructions relating to services which are provided in an infrastructure that is used by several customers of the Processor (shared services), and a change in the processing for individual customers is not possible or is unreasonable.

4.3 The data processing carried out under this Agreement takes place in the United Kingdom or in another contracting state of the Agreement via the European Economic Area, unless the transfer of data to third countries becomes necessary to provide the service. If a transfer to a third country takes place, the processor shall ensure that the relevant Data Protection Legislation requirements are fulfilled, in relation to any such third country transfer.

5. Rights of the Customer, Obligations of the Processor

5.1. The Processor may process data of data subjects only within the framework of the order and the documented instructions of the Customer, except where otherwise required under the applicable Data Protection Legislation (and in such a case shall inform the Customer of that legal requirement before processing, unless applicable Data Protection Legislation prevents it from doing so on important grounds of public interest). This also applies to transfers of personal data to third countries or international organisations. If there is a processing obligation contrary to an instruction, the Processor shall inform the Customer of the relevant legal requirement prior to the processing (unless the relevant law prohibits such information due to an important public interest). The Processor shall inform the Customer without delay if it considers an instruction infringes or may infringe the applicable Data Protection Legislation. The Processor may suspend the implementation of the

instruction until it has been confirmed or modified by the Customer.

5.2. In the light of the nature of the processing, the Processor shall, as far as reasonably possible, assist the Customer with appropriate technical and organisational measures to fulfil the rights of the data subjects laid down in the applicable Data Protection Legislation. The Processor is entitled to demand appropriate compensation from the Customer for these services, unless the support was required due to a breach of law or a breach of contract by the Processor. The Processor shall provide the Customer with cost information in advance.

5.3. Considering the nature of the processing and the information available to the Processor, the Processor shall assist the Customer in its compliance with its obligations as a data controller in respect of data security, data breach notification, data protection impact assessments, prior consultation with supervisory authorities or any notice or investigation by a relevant supervisory authority. The Processor is entitled to demand appropriate compensation from the Customer for these services, unless the support was required due to a breach of law or a breach of contract by the Processor. The Processor shall provide the Customer with cost information in advance.

5.4. The Processor ensures that the employees involved in the processing of Customer's data and other persons acting on behalf of the Processor are prohibited from processing the personal data outside the instruction issued. Furthermore, the Processor ensures that persons authorised to process the personal data are subject to a contractual duty of confidentiality or are under an appropriate statutory obligation of confidentiality. The obligation of confidentiality remains even after the order has been completed.

5.5. The Processor shall inform the Customer immediately if it becomes aware of violations of the protection of personal data of the

Data Processing Terms of Agreement

Customer. The Processor shall take the necessary measures to safeguard the data and to mitigate possible adverse consequences for the data subjects.

5.6. The Processor guarantees the written appointment of a Data Protection Officer, who shall carry out his/her activity in accordance with the applicable Data Protection Legislation. A contact option will be published on the website of the Processor.

5.7. Upon expiry of the provision of the processing services, the Processor will, at the choice of the Customer, either delete or return the personal data, unless there is an obligation under European Union or UK law (as applicable) to retain the personal data, or under any other contractual provision between the parties. If the Customer does not exercise this option, deletion is deemed agreed. If the Customer chooses to return, the Processor can demand reasonable compensation. The Processor shall provide the Customer with cost information in advance.

5.8. If a data subject assert claims for compensation according to the relevant Data Protection Legislation, the Processor shall support the Customer in defending the claims, as far as reasonably possible. The Processor shall be entitled to charge reasonable costs in relation to such assistance.

Data Processing Terms of Agreement

6. Obligations of the Customer

6.1 The Customer must immediately and completely inform the Processor if it identifies errors or irregularities regarding data protection regulations when carrying out the order.

6.2 In the event of termination or expiry of the processing activities, the Customer undertakes to delete any personal data of the Processor which it has stored during the provision of the service, before the termination of the contract.

6.3 At the request of the Processor, the Customer shall appoint a contact person for data protection matters.

7. Requests from the Data Subjects

If the data subject approaches the Processor with requests for correction, deletion or information, the Processor, where possible, shall refer the data subject to the Customer. The Processor shall immediately forward the request of the data subject to the Customer. The Processor shall support the Customer with such requests as far as is reasonably possible. The Processor shall not be liable if the data subject request is not answered by the Customer, not answered correctly or not answered in due time.

8. Measures for the Security of Processing

8.1 The Processor will take appropriate technical and organisational measures in its area of responsibility to ensure that the processing is carried out in accordance with the requirements of the applicable Data Protection Legislation and ensure the protection of the rights and freedoms of the data subjects. The Processor shall take appropriate technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of the processing systems and services in the long term.

Data Processing Terms of Agreement

8.1 The current technical and organisational measures of the processor can be viewed in Clause 13-17.

8.2 The Processor will carry out regular reviews of the effectiveness of the technical and organisational measures to ensure the security of processing in accordance with the relevant Data Protection Legislation.

8.3 The Processor may, because of advances and technical developments or changes to the risk or nature of the processing, in its sole discretion, adapt or implement new measures relating to data security. The Processor shall ensure that any such changes continue to meet the requirements of all applicable Data Protection Legislation.

9. Proof and Verification

9.1 The Processor shall provide the Customer with all information necessary to prove compliance with its data processor obligations and shall allow and contribute to audits, including inspections, carried out by the Customer or another inspector appointed by the Customer (subject always to appropriate obligations of confidentiality). The Processor agrees to the designation of an independent external auditor by the Customer, if the Customer provides the Processor with a copy of the audit report. The Processor may refuse competitors of the Customer or persons working for competitors of the Customer (as may be reasonably determined by the Processor) as investigators.

9.2 The Customer acknowledges and agrees that the Processor's ISO27001 certification demonstrates compliance with certain processor obligations under the relevant Data Protection Legislation. If the Processor ceases to hold ISO27001 certification or in the event of a data breach requiring notification to the relevant supervisory authority, relating to the Customer's personal data, the Customer may perform an audit or inspection of the Processor.

Data Processing Terms of Agreement

9.3 Such inspections may only be carried out during normal business hours and without undue disruption of business. The Customer must give the Processor reasonable notice in writing (unless it is necessary to carry out an inspection without notification, due to a risk of the inspection being jeopardised. The Customer's inspection right is limited to verifying the Processor's compliance with its obligations under the applicable Data Protection Legislation and this Agreement. The Processor will use all reasonable efforts to facilitate and assist the Customer with such inspection.

9.4 The Processor is entitled to charge reasonable costs for the provision of information and assistance, unless the inspection was required due to a breach of law or a breach of contract by the Processor. The Processor shall provide the Customer with cost information in advance.

10. Sub Processors

10.1 The Customer grants the Processor the general permission to use other processors for the fulfilment of the Main Contract (the "**Sub processors**").

10.2 The Sub processors currently used are described in IT-CO/OUR PARTNER(S) Core Sub Processors . By entering into this Agreement, the Customer agrees to their use.

10.3 The Processor shall inform the Customer if it intends to withdraw or replace other Processors. The Customer may object to such changes within 14 days notification by the Processor.

10.4 In the event of an objection, the Processor may choose to provide the service without the intended change or, if the performance of the service without the intended change is not reasonable to the Processor, discontinue the service affected by the change to the Customer within a reasonable time (at least 14 days) after receiving

Data Processing Terms of Agreement

the objection.

10.5 If the Processor engages sub processors, it is the Processor's responsibility to impose its data protection obligations under this Agreement to the sub processor.

10.6 The Processor shall ensure, through regular checks, any sub processors comply with the technical and organisational measures.

11. Liability and Compensation

11.1 In the event of a claim for compensation by a data subject under the applicable Data Protection Legislation, the Parties undertake to assist each other to determine the underlying facts of the claim.

11.2 The liability provision as agreed between the Parties in the Main Contract for the provision of services shall also apply to claims arising from this Agreement and in the internal relationship between the Parties for claims of third parties under the applicable Data Protection Legislation, unless expressly agreed otherwise.

12. Contract Period, Miscellaneous

12.1 The agreement commences on the execution of the Main Agreement by the Customer. It terminates or expires upon the conclusion of the last contract under the respective Customer number. If any data processing on behalf of the Customer continues after termination of this Agreement, the terms of this Agreement remain in force until the processing activities cease.

12.2 The Customer acknowledges this Agreement forms part of the Main Contract concerning the product(s) booked by him. In the event of any conflict between the Main Contract and this Agreement, the provisions of this Agreement shall prevail. Should individually parts of this Agreement be ineffective, this does not affect the validity of the remaining agreements.

Data Processing Terms of Agreement

12.3 The exclusive place of jurisdiction for all disputes arising from and in connection with this Agreement is the registered office of the Processor. This applies subject to any exclusively legal place of jurisdiction. This Agreement is subject to the statutory provisions of English law.

12.4 If the data of the Customer is endangered by seizure or confiscation, by a bankruptcy or settlement procedure, or by other events or measures of third parties, the Processor shall inform the Customer immediately. The Processor will inform all persons responsible in this connection without delay that the sovereignty and the ownership of the data lie exclusively with the Customer qualifying as the controller.

Technical and Organisational Security Measures (version 1.1)

13. Confidentiality

13.1 Entry Control

Unauthorised persons should be denied access to rooms containing data processing equipment. Definition of security areas:

- Realisation of effective access protection.
- Logging of access.
- Determination of persons with access authorisation.
- Management of personal access authorisations.
- Accompaniment of external personnel.
- Monitoring the rooms.

13.2 Login Control

The use of data processing systems by unauthorised persons must be prevented.

- Determination of the protection requirement.
- Login protection.
- Implementation of secure login procedures, strong authentication.

Data Processing Terms of Agreement

- Implementation of simple authentication via username password.
- Logging of login.
- Monitoring of critical IT systems.
- Secure (encrypted) transmission of authentication secrets.
- Blocking in the case of failed attempts/inactivity and process to reset locked login identifiers.
- Ban memory function for passwords and/or form input (server/clients).
- Determination of authorised persons.
- Management and documentation of personal authentication media and login permissions.
- Automatic login lock and manual login lock.

13.3 Access Control

Only the data for which access is authorised can be accessed. Data cannot be read, copied, altered or removed without authorisation during processing, use, and after storage.

- Create an authorisation concept.
- Implementation of access restrictions.
- Assigning minimal authorisations.
- Administration and documentation of personal access rights.
- Avoiding the concentration of roles.

13.4 Usage Purpose Control

It must be ensured that data collected for different purposes can be processed separately.

- Data economy in handling personal data.
- Separate processing of different data sets.
- Regular usage purpose check and deletion.
- Separation of test and development environment.

Data Processing Terms of Agreement

13.5 Privacy-Friendly Presets

If data is not required to achieve the intended purpose, the technical default settings will be set in such a way that data will only be collected, processed, passed on or published by an action of the data subject.

14. Integrity

14.1 Transfer Control

The aim of the transfer control is to ensure that personal data cannot be read, copied, altered or removed during electronic transmission or during its transport or storage on data carriers, and that it is possible to check and determine to which places personal data is provided by means of data transmission.

- Determination of receiving and / or transferring instances / persons.
- Examination of the legality of the transfer abroad.
- Logging of transmissions according to logging concept.
- Secure data transfer between server and client.
- Backup of the transmission in the backend.
- Secure transmission to external systems.
- Risk minimisation through network separation.
- Implementation of security gateways at the network transfer points.
- Hardening of the backend systems.
- Description of the interfaces.
- Implementation of machine-machine authentication.
- Secure storage of data, including backups.
- Secure storage on mobile data carriers.
- Introduction of a disk management process.
- Process for collection and disposal.
- Privacy-compliant deletion and destruction procedures.
- Management of deletion logs.

Data Processing Terms of Agreement

14.2 Input Control

The purpose of the input control is to ensure that it can be subsequently verified and ascertained whether and by whom personal data has been entered, changed or removed in data processing systems.

- Logging of the inputs.
- Documentation of the input permissions.

15. Availability, Resilience, Disaster Recovery

15.1 Availability and Resilience

- Fire protection.
- Redundancy of primary technology.
- Redundancy of the power supply.
- Redundancy of the communication connections.
- Monitoring.
- Resource planning and deployment.
- Defence against systemic abuse.
- Data backup concepts and implementation.
- Regular check of emergency facilities.

15.2 Disaster Recovery - Rapid recovery after incident

- Emergency plan.
- Data backup concepts and implementation.

16. Data Protection Organisation

- Definition of responsibilities.
- Implementation and control of suitable processes.
- Notification and approval process.
- Implementation of training measures.
- Commitment to confidentiality.
- Regulations for the internal distribution of tasks.
- Consideration of role separation and assignment.
- Introduction of a suitable representative scheme.

Data Processing Terms of Agreement

17. Order control

The purpose of order control is to ensure that personal data processed as part of the order can only be processed in accordance with the instructions of the client.

- Selection of other processors for suitable warranties.
- Conclusion of a data processing agreement with other processors.
- Conclusion of a data processing agreement with IT-Co /our Partner(s).

18. Procedure for regular review, assessment and evaluation

- Information security management according to ISO 27001.
- Process for the evaluation of technical and organisational measures.
- Security incident management process.
- Conducting technical reviews.

Revised Date: 18/06/2024