Verwerkersovereenkomst Strato

Data Processing Agreement
According to Art. 28 (3) General Data Protection Regulation (GDPR)
version 3.0

for customer number [74778395]
between

Jan, van Breemen / TOPslaap.nl
Provincialeweg 156
1506 ME Zaandam

as controller
– hereinafter referred to as the client –

and

STRATO AG
Pascalstraße 10
10587 Berlin

as processor
– hereinafter referred to as the processor –

1. **Subject-matter and duration of the processing**
   1.1. The subject matter of the Agreement is the rights and obligations of the parties in the context of the provision of services in accordance with the order, service description and general terms and conditions (hereinafter referred to as the main contract), insofar as the processor processes personal data on behalf of the client as controller according to Art. 28 GDPR. This includes all activities that the processor performs to fulfil the contract and that represent a data processing on behalfof the controller. This also applies if the order does not explicitly refer to this Data Processing Agreement.
   1.2. The duration of the processing corresponds to the term agreed in the order.

2. **Nature and purpose of the processing**
   2.1. The nature of the processing includes all types of processing as defined by the GDPR to fulfil the contract.
   2.2. Purposes of processing are all purposes required to provide the contracted services in terms of cloud services, hosting, Software as a Service (SaaS), and IT support.

3. **Type of personal data and categories of data subjects**
   3.1. The type of processed data is determined by the client by the product selection, the configuration, the use of the services, and the transmission of data.
   3.2. The categories of data subjects are determined by the client via product selection, configuration, the use of the services, and the transmission of data.

4. **Responsibility and processing on documented instructions**
   4.1. The client is solely responsible for complying with the legal requirements of data protection laws, in particular, the legality of the transfer of data to the processor and the legality of data processing under this Agreement (“Responsible” in the sense of Art. 4 no. 7 GDPR). This also applies to the purposes and means of processing set out in this Agreement.
   4.2. The instructions are initially determined by the main contract and can then be changed by the client 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. Instructions that are not provided for in the contract are treated as an application for a change in performance. In the event of proposed changes, the processor shall inform the client 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. Unacceptability exists in particular if the services are provided in an infrastructure that is used by several clients/customers of the processor (shared services), and a change in the processing for individual clients is not possible or is unreasonable.
   4.3. The contractually agreed data processing takes place exclusively in a Member State of the European Union or in another contracting state of the Agreement via the European Economic Area, unless otherwise agreed, e.g. as part of the description of the ordered product.
   4.4. If an integral part of the Contract is the registration of domains with registration offices located in a third country (outside the European Union and the European Economic Area), it is also agreed that the processor will transfer personal data to these registries in compliance with the mandatory regulations.
   4.5. The parties further agree that the processor is entitled to transfer personal data – in compliance with the mandatory provisions for the provision of services in a third country. This is particularly the case if the subject of the Contract is the service of a third party providing this service wholly or partly in a third country.

5. **Rights of the client, 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 client, unless there is an exceptional case within the meaning of Article 28 (3) (a) GDPR (obligation under the law of the European Union or of a Member State). The processor shall inform the client without delay if it considers that an instruction violates applicable laws. The processor may suspend the implementation of the instruction until it has been confirmed or modified by the client.
   5.2. In the light of the nature of the processing, the processor shall, as far as possible, assist the client with appropriate technical and organisational measures in order to fulfil the rights of the data subjects laid down in Chapter III of the GDPR. The processor is entitled to demand appropriate compensation from the client for these services.
   5.3. The processor shall assist the clientin ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GPDR taking into account the nature of processing and the information available to the processor The processor is entitled to demand appropriate compensation from the client for these services.
   5.4. The processor ensures that the employees involved in the processing of the data of the client and other persons acting on behalf of the processor are prohibited from

processing the data outside the instruction issued. Furthermore, the processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The same applies to the secrecy of telecommunications according to § 88 TKG (German Telecommunications Act) and – in knowledge of criminal liability – for the preservation of secrets of professional secrecy according to § 203 StGB (German Penal Code). The obligation of confidentiality/secrecy persists even after the order has been completed.
5.5. The processor shall inform the client immediately if it becomes aware of violations of the protection of personal data of the client. 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 Art. 38 and 39 GDPR. A contact option will be published on the website of the processor .
5.7. At the end of the provision of the processing services, the processor will, at the choice of the client, either delete or return the personal data, unless there is an obligation under European Union or national law to retain the personal data, or something else results under any other contractual arrangements. If the client does not exercise this option, deletion is deemed agreed. If the client chooses return, the processor can demand a reasonable compensation.
5.8. If a data subject asserts claims for compensation according to Art. 82 GDPR, the processor shall support the client in defending the claims within the scope of its possibilities. The processor may require an appropriate remuneration for this.

6. **Obligations of the client**
   6.1. The client must immediately and completely inform the processor if it identifies errors or irregularities with regard to data protection regulations when carrying out the order.
   6.2. In the event of termination, the client undertakes to delete personal data which it has stored during its service, before the termination of the Contract.
   6.3. At the request of the processor, the client appoints a contact person for data protection matters.

7. **Measures for the security of processing according to Art. 32 GDPR**
   7.1. 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 GDPR and ensure the protection of the rights and freedoms of the data subjects. In accordance with Art. 32 GDPR, 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.
   7.2. The current technical and organisational measures are listed in Appendix 2.
   7.3. The processor will operate a procedure for the regular review of the effectiveness of the technical and organisational measures to ensure the security of processing in accordance with Art. 32 (1) lit. d) GDPR.
   7.4. Over time, the processor will adapt the measures taken to developments in the state of the art and the risk situation. A change in the technical and organisational measures taken is reserved to the processor, provided that the level of protection under Art. 32 GDPR is not fallen short of.

8. **Proof and verification**

8.1. The processor shall provide the client with all the information necessary to prove compliance with the obligations laid down in Art. 28 GDPR and shall allow and contribute to audits, including inspections, carried out by the client or another inspector appointed by the client. The processor is entitled to demand a declaration of confidentiality from the client and its appointed auditor. The processor agrees to the designation of an independent external auditor by the client, if the client provides the processor with a copy of the audit report. The processor may refuse competitors of the client or persons working for competitors of the client as investigators.
8.2. As evidence of compliance with the obligations set out in Art. 28 GDPR, the client is required to obtain a ISO 27001 certification. The current certificate is provided by the processor on its website.
8.3. The client's inspection right has the objective of verifying compliance with the obligations incumbent on a processor in accordance with the GDPR and this Contract. Proof of compliance with these obligations is provided by the certification referred to in the preceding paragraph. Insofar as the client asserts legitimate doubts on the basis of factual indications that these certifications are sufficient or appropriate, or if special incidents within the meaning of Art. 33 (1) GDPR in connection with the execution of the data processing on behalf of the client justify this for the client, it may perform inspections. These can be carried out during normal business hours without disruption to the operation after registration, taking into account a reasonable lead time.
8.4. The processor may require reasonable compensation for information and assistance. The cost for the processor through an inspection is always limited to one day per calendar year.
8.5. If a data protection supervisory authority or another state or church supervisory authority of the client carries out an inspection, the above rules apply accordingly. A signing of a confidentiality obligation is not required if this supervisory authority is subject to professional oran appropriate statutory obligation of confidentiality, for which a violation under the German Penal Code is punishable.

9. **Subprocessors (other processors)**

9.1. The client grants the processor the general permission to use other processors within the meaning of Art. 28 GDPR for the fulfilment of the Contract.
9.2. The other processors currently employed are listed in Appendix 1. The client agrees to their engagement.
9.3. The processor shall inform the client if it intends to withdraw or replace other processors. The client may object to such changes.
9.4. The objection to the proposed change can only be raised against the processor for a reason related to a material data protection right within a reasonable time after receipt of the information about the change. 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, provide the service affected by the change to the client within a reasonable time after receipt of the objection.
9.5. If the processor places orders with other processors, it is the processor's responsibility to impose its data protection obligations under this Contract to the other processor.
9.6. Additional processors within the meaning of this regulation are only those other processors who provide services directly related to the provision of the main service.

It does not cover ancillary services related to telecommunications, printing/postal/transport services, maintenance and service, user services or the disposal of data media and other measures to ensure the confidentiality, availability, integrity and resilience of personal data, networks, services, data processing systems and other IT systems. However, in order to ensure data protection and data security with respect to the data of the client, the processor is obliged to take appropriate and legally compliant contractual agreements as well as control measures for such ancillary services.

10. **Liability and compensation**
    10.1. In the case of assertion of a claim for compensation by a data subject person pursuant to Art. 82 GDPR, the parties undertake to support each other and to contribute to the clarification of the underlying facts.
    10.2. The liability regulation agreed between the parties in the main contract for the provision of services shall also apply to claims arising from this Data Processing Agreement and in the internal relationship between the parties for claims of third parties under Art. 82 GDPR, unless expressly agreed otherwise.

11. **Contract period, miscellaneous**
    11.1. The agreement begins with the conclusion by the customer. It ends with the end of the last Contract under the above-mentioned customer number. If any data processing on behalf of the client still takes place after termination of this contract, the regulations of these agreements are valid until the actual end of the processing.
    11.2. The processor may change the Agreement at its reasonable discretion with reasonable notice. Clause 1.4 of the general terms and conditions applies.
    11.3. In addition, the general terms and conditions of the processor, available at https://www.strato.de, also apply. In the event of any contradictions, the provisions of this Agreement for data processing shall prevail to the provisions of the main contract. Should individual parts of this Agreement be ineffective, this does not affect the validity of the remaining agreements.
    11.4. The exclusive place of jurisdiction for all disputes arising from and in connection with this contract is Berlin. This applies subject to any exclusively legal place of jurisdiction. This Contract is subject to the statutory provisions of the Federal Republic of Germany.
    11.5. If the data of the client 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 client 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 client as the “responsible party” within the meaning of the GDPR.

Appendix 1 to the Data Processing Agreement – Approved subprocessors/additional processors

Date 20180327

Subprocessor	Country	Address	Brief description of the service
Content Management AG	Germany	Im Medienpark 6, 50670 Köln	Development and maintenance of the website builder

Subprocessor	Country	Address	Brief description of the service
ePages GmbH	Germany	Pilatuspool 2, 20355 Hamburg	Development and maintenance of the webshops
Open-Xchange GmbH	Germany	Martinstraße 41, 57462 Olpe	Development and maintenance of the communicator
1&1 Internet SE	Germany	Elgendorfer Straße 7, 56410 Montabaur	Development and operation of the STRATO online accounting tool
Seven IT GmbH	Germany	SevenIT, Hauptstraße 40, 77652 Offenburg	Operation and support of the STRATO online accounting tool

Appendix 2 to the Data Processing Agreement – Technical and organisational security measures according to Art. 32 GDPR
version 1.0

1. **Confidentiality (Article 32 (1) (b) GDPR)**
1.1 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
1.2 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
• 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
1.3 Access Control
Only the data for which access is authorised can be accessed. Data can not 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
1.4 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
1.5 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.

2. **Integrity (Article 32 (1) (b) GDPR)**
2.1 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/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
2.2 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

3. **Availability, resilience, disaster recovery**
   3.1 Availability and resilience (Article 32 (1) (b) GDPR)
   • 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
   3.2 Disaster Recovery – Rapid recovery after incident (Article 32 (1) (c) GDPR)
   • Emergency plan
   • Data backup concepts and implementation

4. **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

5. **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 an data processing agreement with other processors
   • Conclusion of an data processing agreement with STRATO

6. **Procedure for regular review, assessment and evaluation (Article 32 (1) (d) GDPR, Article 25 (1) GDPR)**
   • Information security management according to ISO 27001
   • Process for the evaluation of technical and organisational measures
   • Security incident management process
   • Conducting technical reviews

Je hebt op 20-05-2018 een verwerkersovereenkomst afgesloten met STRATO.