Productsup

Agreement

Between the responsible person/client:

Sample Company, Sample Street, Sample City

- hereinafter referred to as customer (CU) - and the processor:

Products Up GmbH, Alex-Wedding-Str. 5, 10178 Berlin, Germany

- hereinafter referred to as contractor (CO) - the following data processing agreement is made.

Preamble

This agreement is concluded in compliance with the Federal Data Protection Act (BDSG) and the EU General Data Protection Regulation (GDPR) valid from 25.05.2018 as well as with all other relevant data protection regulations. This agreement is governed by the current laws, as amended from time to time.

This agreement concerns the collection, processing and use of personal data in the sense of the BDSG and GDPR by the contractor on behalf of the client ("order processing"). Personal data are individual details about personal or factual circumstances of a specific or identifiable natural person ("data subject"). The agreement deals with the processing of personal data ("order data").

Against this background, the parties agree as follows:

1. Subject and duration of the contract

(1) Subject

      The main subject of the contract for the handling of data is the performance of the following tasks by the contractor: Provision of a cloud-based Data-Feed-Management-Platform for maintenance and optimization of contractor's data.

(2) Duration

The duration of this contract (term) is the duration of the service level agreement.

2. Specification of the content of the order

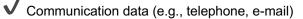(1) Nature and purpose of the intended processing of data

The nature and purpose of the processing of personal data by the contractor for the client are specifically described in the service agreement.

The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another Contracting State to the Agreement on the European Economic Area. Any transfer to a third country requires the prior consent of the client and may only take place if the special requirements of art. 44 et seq. GDPR are met.

(2) Type of data

The subject of the processing of personal data is the following data types/categories (enumeration/description of the data categories)

    ✔ Person master data (contact list of the working group, i.d.R no data subject)

    ✔ Communication data (e.g., telephone, e-mail)

    ✔ Contract master data (contractual relationship, product or contract interest)

✔ Billing and payment data

(3) Categories of data subjects

The categories of persons affected by processing include:

✔ Employees of the client

✔ Suppliers   and   partners   of   the   client

3. Technical-organizational measures

(1) The contractor must document the implementation of the technical and organizational measures set out prior to the award of the contract and prior to processing, in particular with regard to the specific execution of the order, and hand them over to the client for review. If accepted by the client, the documented measures become the basis of the contract. Insofar as the inspection/audit of the client results in a need for adjustment, this must be implemented by mutual agreement.

(2) The contractor has to establish security according to art. 28 para. 3 lit. c, 32 GDPR, in particular in conjunction with art. 5 para. 1, para. 2 GDPR. Overall, the actions to be taken are data security measures and to ensure a level of protection appropriate to the level of risk with regard to the confidentiality, integrity, availability and resilience of the systems. In this context, the state of the art, the costs of implementation and the nature, scope and purpose of the processing as well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of art. 32 para. 1 GDPR must be taken into account. [See details in attachment 1].

(3) The technical and organizational measures are subject to technical progress and further development. In that regard, the contractor is allowed to implement alternative adequate measures. In doing so, the safety level of the specified measures must not be undershot. Significant changes must be documented.

4. Correction, restriction and deletion of data

(1) The contractor may not correct, delete or restrict the processing of the data processed on behalf of the contract, only on the basis of documented instructions from the client. Insofar as an affected person directly addresses the contractor in this regard, the contractor will immediately forward this request to the client.

(2) Insofar as included in the scope of services, the cancellation concept, the right to be forgotten, rectification, data portability and information according to the client's documented instructions are to be ensured by the contractor directly.

(3) The contractor shall support the customer within the scope of his possibilities, if agreed upon. persons affected by the fulfilment of enquiries and claims pursuant to Chapter III of the GDPR and compliance with the obligations set out in Art. 33 to 36 GDPR.

5. Quality assurance and other obligations of the contractor

In addition to compliance with the provisions of this order, the contractor has statutory obligations according to art. 28 to 33 GDPR; In particular, he ensures compliance with the following requirements:

   a) Written appointment of a data protection officer who carries out his activity in accordance with art. 38 and 39 GDPR. As an external data protection officer is:

   Nils Möllers, Keyed GmbH, Siemensstraße 12, 48341 Altenberge, n.moellers@keyed.de
   appointed to the contractor. A change of the data protection officer has to be told the client immediately.

b) The preservation of confidentiality under art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. The contractor will use only employees who are committed to confidentiality and who have been previously familiarized with the data protection regulations that are relevant to them. The contractor and any person subordinate to the contractor who has access to personal data may process such data only in accordance with the instructions of the client, including the powers granted in this contract, unless they are required by law to process them.

c) The implementation and compliance with all technical and organizational measures required for this contract in accordance with art. 28 para. 3 sentence 2 lit. c, 32 GDPR [details in attachment 1].

d) The client and the contractor cooperate with the supervisory authority on request to fulfill their duties.

e) Immediate information to the client about control actions and measures of the supervisory authority, insofar as they relate to this order. This also applies insofar as a competent authority has determined in the context of an administrative or criminal procedure with regard to the processing of personal data in the processing of orders by the contractor.

f) Insofar as the client himself is subject to inspection by the supervisory authority, an administrative offense or criminal proceeding, the liability claim of a data subject or a third party or any other claim in connection with order processing by the contractor, the contractor shall support him to the best of his ability.

g) The contractor shall regularly review the internal processes as well as the technical and organizational measures to ensure that the processing in its area of responsibility complies with the requirements of applicable data protection law and that the protection of the data subject's rights is ensured.

h) verifiability of the technical and organizational measures taken towards the client within the scope of his control powers according to section 7 of this contract.

i) The contractor shall, in accordance with the instructions of the Client, take reasonable measures to prevent further unlawful disclosure by third parties and/or to avert further impairments by the parties concerned. The Supplier shall take all necessary measures to secure data and minimise damage until any instructions have been given by the Customer.

j) The contractor shall support the Customer in complying with its legal obligations, in particular obligations to ensure the security of personal data, reporting obligations in the event of data breakdowns, information obligations vis-à-vis affected parties and supervisory authorities, data protection impact assessments and prior consultations. The same shall also apply if the client is subject to inspection by the supervisory authority, administrative offence or criminal proceedings, the liability claim of a person concerned or a third party or any other claim in connection with order processing. Upon request, the Contractor shall make available to the Client the list of all processing activities to be carried out by the Contractor in copied form in accordance with the relevant legal provisions.

k) The contractor shall inform the contracting authority without delay if he becomes aware of any infringement of the protection of personal data of the contracting authority. The Contractor shall take the necessary measures to secure the data and to reduce possible negative consequences for the persons concerned and shall consult with the Customer without delay.

6. Subcontracting

(1) For the purposes of this regulation, subcontracting means such services which directly relate to the provision of the main service. This does not include ancillary services provided by the contractor, e.g.

as a telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing facilities. However, the contractor is obliged to take appropriate and legally compliant contractual agreements and control measures in order to ensure data protection and data security of the client's data, even with outsourced ancillary services.

(2) The contractor may only commission subcontractors (other processors) after prior express written consent from the client.

a) ☐ Subcontracting is prohibited.

b) ☒ The client agrees to the assignment of the following subcontractors under the condition of a contractual agreement in accordance with art. 28 para. 2-4 GDPR:

Company subcontractor	Address/Country	Service
Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109 United States	Cloud Services for Server and Data Hosting
Hetzner Online GmbH	Industriestr. 25 91710 Gunzenhausen Deutschland	Web Hosting and Data Center Provider
Google LLC	1600 Amphitheatre Parkway Mountain View, CA 94043 USA	Cloud Services for Server and Data Hosting
firstcolo GmbH	Kruppstraße 105, 60388 Frankfurt am Main Deutschland	Web Hosting and Data Center Provider
Productsup B.V.	Emmaplein 4, D5211VW 'sHertogenbosch	Affiliate software provider

c) ☒ The outsourcing to subcontractors or / the change of the existing subcontractor are permissible insofar as:

- the contractor indicates such outsourcing to subcontractors at least 2 weeks in advance in writing or in text form, and
- the client does not object to the planned outsourcing in writing or in text form until the date of transfer of the data to the contractor and
- a contractual agreement in accordance with art. 28 para. 2-4 GDPR is used.

(3) The transfer of personal data of the client to the subcontractor and its initial action shall only be permitted upon submission of all conditions for subcontracting.

(4) If the subcontractor provides the agreed service outside the EU/EEA, the contractor shall ensure that the data protection law is admissible by taking appropriate measures. The same applies if service providers within the meaning of para. 1 sentence 2 are to be used.

(5) Further outsourcing by the subcontractor

☐ is not allowed;

☐ requires the explicit consent of the main client (at least in text form);

☒ requires the express consent of the main contractor (at least in text form);

All contractual arrangements in the chain of contract must also be imposed on the additional subcontractor.

7. Control rights of the client

(1) The client has the right to carry out inspections in consultation with the contractor or to have them carried out by examiners to be named in individual cases. He has the right to satisfy himself of the compliance of this agreement by the contractor in his business through spot checks, which are usually timely to register.

(2) The contractor shall ensure that the client can satisfy himself of the compliance with the obligations of the contractor in accordance with art. 28 GDPR. The contractor undertakes to provide the client with the necessary information upon request and, in particular, to prove the implementation of the technical and organizational measures.

(3) The proof of such measures, which do not concern only the concrete order, can take place for example by

- the compliance with approved codes of conduct pursuant to art. 40 GDPR;
- the certification according to an approved certification procedure according to art. 42 GDPR;
- up-to-date certificates, reports or statements of independent bodies (e.g. auditors, data protection officers, IT security departments, privacy auditors, quality auditors);
- the appropriate certification through IT security or privacy audit (e.g. according to BSI basic protection).

(4) The contractor may assert a claim for compensation in order to allow controls by the client.

8. Notification in case of violations of the contractor

(1) The contractor supports the client in compliance with art. 32-36 of the GDPR data security obligations, reporting of data breaches, data protection impact assessments and prior consultations. These include

a) ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing and the predicted likelihood and severity of a possible breach of rights through vulnerabilities, and enable the immediate detection of relevant injury events

b) the obligation to report violations of personal data immediately to the client

c) the obligation to assist the contracting entity in providing information to the person concerned, and to provide him with all relevant information without delay in that connection

d) the support of the client for its data protection impact assessment

e) the assistance of the contracting authority in the context of prior consultations with the supervisory authority

(2) For services that are not included in the terms of reference or that are not the result of a wrongdoing by the contractor, the contractor may claim a fee.

(3) For support services which are not included in the service description or are not due to a misconduct of the contractor, the contractor can claim a remuneration if the expenses exceed the number of 2 audits per year.

(4) The contractor shall be liable to the Client for the subcontractor's compliance with the data protection obligations imposed by the Contractor in accordance with this Section of the Contract. Liability is governed by the provisions of Art. 82 GDPR.

(5) The contractor's legal representatives or vicarious agents shall not be liable for slight negligence. However, this exclusion of liability for slight negligence shall not apply in the event of a breach of a

material contractual obligation (cardinal obligation). Cardinal obligations or essential contractual obligations are such obligations of the contractor, the fulfilment of which makes the proper execution of this concrete contract possible in the first place and on the observance of which the customer may regularly rely; i.e. obligations, the breach of which would endanger the achievement of the purpose of the contract.

9. Authorization of the client

The client alone has the authority to decide or issue instructions for order processing. The Contractor shall act solely on behalf of and in the interest of the Client. The responsibility for compliance with the data protection law and the legality of the order processing as well as for the protection of the rights of the parties concerned lies with the client.

The Contractor shall carry out the order processing exclusively within the framework of the agreement and according to written instructions of the Customer, whereby the instructions shall have priority, or if there is a legal obligation to process. Oral instructions shall be confirmed by the client in writing without delay. The contractor is not entitled to make declarations to the parties concerned without the prior written consent of the client. In the event of a statutory obligation, the Contractor shall notify the Customer of this obligation prior to processing.

The Contractor may not correct, delete or restrict the processing of the order data without the Customer's authorization, but only in accordance with the Customer's instructions in writing. The Contractor shall immediately inform the Customer in writing about all inquiries and complaints of the parties concerned and support the Customer in safeguarding the rights of the parties concerned, e.g. by notification, provision of information or correction, blocking and deletion of order data.

The parties shall observe the relevant data protection regulations within the scope of order processing. If the contractor is of the opinion that an agreement or instruction violates data protection regulations, he will inform the client immediately in writing. The contractor is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the client.

(1) Oral instructions shall be confirmed by the Customer without delay (at least in text form).

(2) The contractor shall inform the customer immediately if he is of the opinion that an instruction violates data protection regulations. The contractor is entitled to suspend the execution of the corresponding instruction until it has been confirmed or changed by the client.

10. Deletion and return of personal data

(1) Copies or duplicates of the data are not created without the knowledge of the client. This does not include backup copies, to the extent necessary to ensure proper data processing, and data required for compliance with statutory retention requirements.

(2) After the conclusion of the contractually agreed work or sooner upon request by the client - at the latest upon termination of the service agreement - the contractor shall have all documents, processing results and utilization results as well as data sets which are related to the contract relationship to hand over client or to destroy it after prior consent in accordance with data protection. The same applies to test and scrap material. The log of the deletion must be submitted on request.

(3) Documentation serving as proof of orderly and proper data processing shall be kept by the contractor according to the respective retention periods beyond the end of the contract. He can hand them over to the client for his discharge at the end of the contract.

11. Secrecy

The contractor will keep the information and documents received in the course of the order processing, in particular the order data, strictly confidential ("business and trade secrets"). The confidentiality obligations shall continue to apply indefinitely even after termination of this agreement.

The duty to maintain secrecy shall not apply or shall cease to exist if the information and documents were already known to the public or the contractor upon conclusion of this agreement or became known to the public after conclusion of this agreement, without the contractor being at fault, or if the contractor is known to a third party, provided the third party does not breach its own confidentiality obligation when handing over the information. The contractor is liable for these facts.

12. Miscellaneous, General

Changes and additions to this agreement and any of its components, including any warranties of the contractor require a written agreement and the explicit reference to the fact that it is a change or supplement of these terms. This also applies to the waiver of this form requirement.

Should the Client's data be endangered by seizure or confiscation by the Contractor, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall immediately inform the Client thereof.

The Contractor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Customer as the person responsible within the meaning of the Basic Data Protection Regulation.

Amendments and supplements to this Annex and all its components - including any assurances by the Contractor - shall require a written agreement, which may also be made in an electronic format (text form), and an express reference to the fact that these Terms and Conditions have been amended or supplemented. This also applies to the waiver of this formal requirement.

In the event of any contradictions, the provisions of this annex on data protection shall take precedence over the provisions of the contract. Should individual parts of this appendix be invalid, this shall not affect the validity of the remainder of the appendix.

Jurisdiction is Berlin.

Attachment 1 - Technical and organizational activities

If not applicable, please delete. If necessary, please complete further activities.

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

- Physical access control
  No unauthorized access to data processing systems, for example: magnetic or chip cards, keys, electric strikes, security or gatekeepers, alarm systems, video systems;

- System access control
  No unauthorized system usage, such as: (secure) passwords, automatic locking mechanisms, two-factor authentication, disk encryption;

- Data access Control
  No unauthorized reading, copying, modification or removal within the system, for example: authorization concepts and needs-based access rights, logging of accesses;

- Separation Control
  Separate processing of data collected for different purposes, e.g. Multi-client capability, sandboxing;

- Pseudonymisation (Article 32 para. 1 lit. a of the GDPR; article 25 para. 1 of the GDPR)
  The processing of personal data in such a way that the data can no longer be assigned to a specific data subject without the need for additional information, provided that such additional information is kept separate and subject to appropriate technical and organizational measures;

2. Integrity (Article 32 para. 1 lit. b of the GDPR)

- Relay control
  No unauthorized reading, copying, modification or removal during electronic transmission or transport, for example: encryption, Virtual Private Networks (VPN), electronic signature;

- Entry Control
  Determining if and by whom personal data has been entered, altered or removed in data processing systems, e.g. logging, document management;

3. Availability and resilience (Article 32 para. 1 lit. b GDPR)

- Availability Control
  Protection against accidental or willful destruction or loss, such as: on-site/off-site backup strategy, uninterruptible power supply (UPS), antivirus, firewall, reporting and contingency plans;

- Rapid recoverability (Article 32 para. 1 lit. c GDPR);

4. Procedures for regular review and evaluation (Article 32 para. 1 lit. d GDPR), Article 25 para. 1 of the GDPR)

- Privacy Management;

- Incident-Response-Management;

- Privacy-friendly default settings (Article 25 para. 2 GDPR);

- Order control
  No order data processing within the meaning of Art. 28 GDPR without corresponding instructions of the client, for example: Clear contract design, formalized order management, strict selection of the service provider, compulsory pre-compilation, follow-up checks.