

Data Processing Agreement according to Art. 28 para. 3 GDPR

between

– Controller, hereinafter referred to as the "**Client**" –

and the

Cloud86 B.V., Lavendelheide 21-108, 9202 PD Drachten, Netherlands

– Processor, hereinafter referred to as the "**Contractor**" –

– individually and/or collectively hereinafter referred to as the '**Contracting Party**' or '**Party(s)**',

1. Subject matter and duration of the agreement

- 1 The order, the specific description of the service and the duration are regulated in **Annex 1**.
- 1 The Contractor processes personal data for the Client within the meaning of Art. 4 No. 2 and Art. 28 GDPR on the basis of this contract.
- 1 The contractually agreed service is provided exclusively in a member state of the European Union or in a state party to the Agreement on the European Economic Area. Any relocation of the service or parts of the work thereof 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 (e.g. adequacy decision of the Commission, standard data protection clauses (possibly with additional technical security measures), approved rules of conduct).
- 1 The Client may terminate the contract at any time without notice if there is a serious breach by the Contractor of data protection regulations or the provisions of this contract, if the Contractor cannot or does not want to carry out an instruction of the Client, or if the Contractor denies the Client's control rights in breach of the contract or if obligations derived from Art. 28 GDPR are violated.

2. Type and purpose of the processing, type of personal data and categories of data subjects:

- 2 Details on the type of processing (pursuant to Art. 4 No. 2 GDPR), the type of personal data (pursuant to Art. 4 No. 1, 13, 14 and 15 GDPR) and categories of data subjects (pursuant to Art. 4 No. 1 GDPR) can also be found in **Annex 1**.

3. Rights and obligations as well as authority of the client

- 3 The Client is solely responsible for assessing the permissibility of the processing in accordance with Art. 6 (1) GDPR and for safeguarding the rights of the data subjects under Art. 12 to 22 GDPR. Nevertheless, the Contractor is obliged to forward all such inquiries to the Client without delay, provided that they are recognisably addressed exclusively to the Client.
- 3 Changes to the regulatory content of **Annex 1** and procedural changes must be jointly agreed between the client and the contractor and determined in writing or in an electronic format.
- 3 As a rule, the Client issues all orders, partial orders and instructions in writing or in a documented electronic format. Verbal instructions must be confirmed immediately in writing or in a documented electronic format.
- 3 The Client shall be entitled to satisfy itself of compliance with the technical and organisational measures taken by the Contractor as well as the obligations set out in this Agreement, in particular in accordance with Section 5 of this Agreement, prior to the commencement of processing and then regularly to an appropriate extent or through third parties. The persons entrusted with the inspection must be given access and insight by the contractor to the extent necessary. If a third party obliged by the Client to carry out an audit is in a competitive relationship with the Contractor, the Contractor shall have a right of objection against the Contractor. The Contractor is obliged to provide the necessary information, demonstrate processes and provide evidence that is necessary to carry out an inspection within the framework of the instruction relationship.
- 3 Inspections shall take place with reasonable notice and during the Contractor's business hours, and no more frequently than every 12 months. Insofar as the Contractor provides proof of the correct implementation of the agreed data protection obligations of this contract, an inspection shall be limited to random samples. Regulations on any remuneration for additional expenses incurred by the support in carrying out an inspection at the contractor beyond the scope described above shall remain unaffected.
- 3 The Client shall inform the Contractor immediately if it discovers any errors or irregularities in the examination of the results of the contract.

4. Authorized Persons of the Client, Recipients of Instructions of the Contractor

- 4 The details of this are also **set out in Annex 4**.
- 4 In the event of a change or a long-term inability to use the contact persons, the successors or representatives must be notified to the respective contractual partner immediately and in principle in writing or electronically.

5. Obligations of the Contractor

- 5 The Contractor shall process personal data exclusively within the framework of the agreements made and in accordance with instructions (Section 3.3 of this Agreement) of the Client, unless the Client is obliged to carry out any other processing by Union or Member State law to which the Client is subject (e.g. investigations by law enforcement or state security authorities); in such a case, the Contractor shall inform the Client of these legal requirements prior to processing, unless the relevant law prohibits such notification on the grounds of an important public interest (Art. 28 (3) sentence 2 lit. a GDPR).
- 5 The Contractor shall not use the personal data provided for processing for purposes other than those regulated in **Annex 1** , in particular not for its own purposes. Copies or duplicates of personal data will be made only with the consent of the Client.
- 5 The Contractor shall ensure that all agreed measures will be carried out in accordance with the contract in the area of the processing of personal data in accordance with the contract. He assures that the data processed for the client will be strictly separated from other databases.
- 5 If available, the data carriers that originate from the Client or are used for the Client are specially marked. Incoming and outgoing as well as ongoing use are documented.
- 5 The Contractor is responsible for the entire execution of his service for the Client. In particular, he must carry out and document regular inspections in his area.
- 5 The Contractor must cooperate to the extent necessary in the fulfilment of the rights of data subjects under Art. 12 to 22 GDPR by the Client, in the preparation of the records of processing activities (Art. 30 GDPR) and in the necessary data protection impact assessments (Art. 35 GDPR) of the Client and provide the Client with appropriate support as far as possible (Art. 28 para. 3 sentence 2 lit. e and f GDPR). He must forward the information required for this purpose immediately to the following department of the client:

6. Instructions

- 6 The Contractor shall immediately draw the Client's attention to this if, in its opinion, an instruction issued by the Client violates statutory provisions (Art. 28 para. 3 sentence 3 GDPR). The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller at the Client after review.
- 6 The Contractor shall correct, delete or restrict the processing of personal data from the contractual relationship if the Client requests this by means of an instruction and the Contractor's legitimate interests do not conflict with this.
- 6 The Contractor may only provide information about personal data from the contractual relationship to third parties or the person concerned after prior instruction or consent by the Client.
- 6 The Contractor agrees that the Client is entitled – in principle by appointment – to monitor compliance with the provisions on data protection and data security as well as the contractual agreements to an appropriate and necessary extent itself or through third parties commissioned by the Client, in particular by obtaining information and inspecting

the stored data and the data processing programs, as well as by on-site inspections and inspections (Art. 28 para. 3 sentence 2 lit. h GDPR).

- 6 The Contractor warrants that it will assist in these inspections where necessary.
- 6 The processing of data in private homes (teleworking or working from home by employees of the Contractor) is permitted only with the consent of the Client. If the data is processed in a private home, access to the employee's home must be contractually ensured beforehand for the employer's control purposes. The measures pursuant to Art. 32 GDPR must also be ensured in this case.
- 6 The Contractor confirms that it is aware of the data protection provisions of the GDPR that are relevant to order processing.
- 6 The Contractor undertakes to maintain confidentiality in the processing of the Client's personal data in accordance with the order. This continues even after the termination of the contract.
- 6 The Contractor assures that it familiarizes the employees employed in the execution of the work with the provisions of data protection that apply to them before commencing work and obliges them to maintain confidentiality in an appropriate manner for the duration of their work as well as after the termination of the employment relationship (Art. 28 para. 3 sentence 2 lit. b and Art. 29 GDPR). The Contractor shall monitor compliance with data protection regulations in its company.
- 6 A company data protection officer has not been appointed by the contractor, as the legal necessity for an appointment does not exist. The contact person at the contractor is named in **Annex 1**.
- 6 The Contractor undertakes to inform the Client immediately of the revocation of a certification in accordance with Art. 42 (7) GDPR.
- 6 Instructions of the Client shall be retained for their period of validity and thereafter for three (3) full calendar years.

7. Obligations of the Contractor to notify in the event of disruptions to processing and personal data breaches

The Contractor shall immediately inform the Client of any disruptions, violations by the Contractor or the persons employed by the Contractor, as well as of any data protection provisions or the stipulations made in the Order, as well as of any suspicion of data protection violations or irregularities in the processing of personal data. This applies in particular with regard to any reporting and notification obligations of the client under Art. 33 and Art. 34 GDPR. The Contractor undertakes to provide the Client with appropriate support in its obligations under Art. 33 and 34 GDPR if necessary (Art. 28 para. 3 sentence 2 lit. f GDPR). The Contractor may only carry out reports pursuant to Art. 33 or 34 GDPR for the Client after prior instructions in accordance with Section 4 of this contract.

8. Subcontracting relationships with subcontractors (Art. 28 para. 3 sentence 2 lit. d GDPR)

- 8 The Contractor is only permitted to commission subcontractors to process the Client's data with the consent of the Client, Art. 28 (2) GDPR, which is carried out via one of the

above-mentioned communication channels (No. 4.) with the exception of oral permission. Consent can only be given if the contractor informs the client of the name and address as well as the intended activity of the subcontractor. In addition, the contractor must ensure that it carefully selects the subcontractor, taking into account in particular the suitability of the technical and organisational measures taken by the subcontractor within the meaning of Art. 32 GDPR. The relevant test documents shall be made available to the Client upon request.

- 8 Subcontractors may only be commissioned in third countries if the special requirements of Art. 44 et seq. GDPR are met (e.g. adequacy decision of the Commission, standard data protection clauses, approved rules of conduct).
- 8 The Contractor must contractually ensure that the agreed provisions between the Client and the Contractor also apply to subcontractors. In the contract with the subcontractor, the information must be specified in such a way that the responsibilities of the contractor and the subcontractor are clearly delineated. If several subcontractors are used, this also applies to the responsibilities between these subcontractors. In particular, the client must be entitled, if necessary, to carry out appropriate checks and inspections, including on site, at subcontractors or to have them carried out by third parties commissioned by him.
- 8 The contract with the subcontractor must be drawn up in writing, which can also be done in an electronic format (Art. 28 para. 4 and para. 9 GDPR).
- 8 The forwarding of data to the subcontractor is only permissible if the subcontractor has fulfilled the obligations under Art. 29 and Art. 32 para. 4 GDPR with regard to its employees.
- 8 The Contractor shall verify compliance with the obligations of the subcontractor(s). The result of the inspections must be documented and made available to the client on request.
- 8 The Contractor shall be liable to the Client for the subcontractor's compliance with the data protection obligations contractually imposed on it by the Contractor in accordance with this section of the Agreement.
- 8 At present, the subcontractors designated in **Annex 2** by name, address and the content of the contract are engaged in the processing of personal data to the extent specified therein. The Client agrees to commission them.
- 8 The Contractor shall always inform the Controller of any intended change with regard to the use of new subcontractors or the replacement of existing ones, which shall give the Client the opportunity to object to such changes (Section 28 (2) sentence 2 GDPR).

9. Technical and organisational measures in accordance with Art. 32 GDPR (Art. 28 para. 3 sentence 2 lit. c GDPR)

- 9 A level of protection appropriate to the risk to the rights and freedoms of the natural persons affected by the processing is guaranteed for the specific order processing. To this end, the protective objectives of Art. 32 (1) GDPR, such as confidentiality, integrity and availability of the systems and services as well as their resilience with regard to the type, scope, circumstances and purpose of the processing, are taken into account in

such a way that the risk is contained in the long term by appropriate technical and organisational remedial measures.

- 9 In order to ensure that processing complies with data protection regulations, the Contractor shall bindingly regulate its procedures for regularly reviewing, evaluating and evaluating the effectiveness of the technical and organisational measures.
- 9 The Contractor shall provide evidence of the technical and organisational measures by means of the completed checklist in accordance with **Annex 3**.
- 9 Decisions on the organisation of data processing and the procedures used that are relevant for security purposes must be agreed between the contractor and the client.
- 9 If the measures taken by the Contractor do not meet the requirements of the Client, the Client shall notify the Client immediately.
- 9 The measures at the contractor can be adapted to technical and organizational development in the course of the contract relationship, but must not fall below the agreed standards.
- 9 The Contractor must coordinate significant changes with the Client in documented form (in writing, electronically). Such votes shall be retained for the duration of this contract.

10.Obligations of the Contractor after termination of the assignment, Art. 28 (3) sentence 2 (g) GDPR

- 1 After completion of the contractual work, the Contractor shall either hand over to the Client at the Client's discretion all data, documents and processing or usage results that have come into its possession as well as to subcontractors, as well as copies that are in connection with the contractual relationship, or delete them in accordance with data protection regulations or have them destroyed and/or have them destroyed. The destruction must be carried out in such a way that it is no longer possible to restore even residual information with reasonable effort. This obligation does not exist if there is an obligation to store the data under Union law or applicable national law, which includes, in particular, retention obligations under tax law or commercial balance sheets.
- 1 In the event of deletion or destruction, the Client must be confirmed in writing or in a documented electronic format with the date.
- 1 Documentation that serves to prove proper data processing must be retained by the Contractor even after the end of the contract in accordance with the respective retention periods. He can hand them over to the client at the end of the contract to relieve him.

11.Liability

- 1 Art. 82 GDPR applies to the liability of the contracting parties.
- 1 If the Contractor is solely responsible in accordance with Art. 82 (2), sentence 2 GDPR, it shall indemnify the Client against claims for damages by third parties.

12.Final provisions

- 12.1. The following annexes are an integral part of this contract:
 - Annex 1** Supplement to the Data Processing Agreement
 - Annex 2** Approved subcontractors

Annex 3 TOM

Annex 4 Persons authorised to issue instructions

The annexes can be customized; the new version automatically becomes part of the agreement.

- 1 Any previous agreements between the contracting parties on the data processing order pursuant to Section 11 of the Federal Data Protection Act (BDSG) shall be cancelled and replaced by this order processing agreement pursuant to Article 28 (3) of the GDPR.
- 1 Amendments or additions to this Agreement must be made in writing or by means of electronic format. This also applies to a waiver of this written form requirement. There are no oral ancillary agreements.
- 1 Agreements on the technical and organizational measures as well as control and audit documents (also on subcontractors) must be retained by both contracting parties for the duration of the order processing and thereafter for three (3) full calendar years.
- 1 If the property or the personal data of the Client to be processed by the Contractor are endangered by measures taken by third parties (e.g. by seizure or seizure), by insolvency or composition proceedings or by other events, the Contractor must inform the Client immediately.
- 1 The right of retention or any other right to withhold performance is excluded with regard to the personal data processed for the Client and the associated data carriers.
- 1 Should individual provisions of this agreement be or become invalid, the validity of the remaining provisions shall not be affected.

[Client's company]

Date / Authorized Signature

Date / Authorized Signature

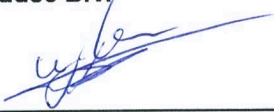
Name (in block letters)

Name (in block letters)

Title

Title

Cloud86 B.V.



Authorized Signature

Maurice Graber

Name (in block letters)

Director

Title

Annex 1 Supplement to the Data Processing Agreement

Subject matter and purpose of the contract:	Type of data processed:	Circle of those affected:	Duration of the job:
<ul style="list-style-type: none"> • Hosting of websites and related technical services. • Customer verification to prevent fraud and to verify identity, using customer data from WHMCS (email address, customer number, and contact details). • Telephone support, including the temporary recording and storage of phone calls for up to 30 days for quality, security, and training purposes. • Processing of textual content for the purpose of translations and document quality in a restricted paid version of ChatGPT (OpenAI), for internal use only. 	<p>For example:</p> <ul style="list-style-type: none"> • Personal data • Communication data (e.g. phone number, email address, IP address, cookie ID, browser/device data) • Contract data • Customer history • Payment and billing data • Planning and control data • Verification data (such as email address from WHMCS, customer number) • Call recordings (retention period: max. 30 days) • Telephone metadata (e.g. date, time, duration) 	<ul style="list-style-type: none"> • Customers • Prospective customers • Subscribers • Employees • Suppliers • Individuals who contact the support department (by phone or through other channels) 	<p>For the duration of the contractual relationship between the parties</p>

Annex 2: Approved subcontractors

1. Damien Overeem
 - Address: Buitenweg 95, 8414 MC Nieuwehorne
 - Activities: Software development, maintenance, and technical support for Cloud86 systems, including access to production environments in which personal data is processed.
 - Type of processing: Access to and processing of personal data for technical analysis, troubleshooting, and further development of systems.
2. OpenAI (ChatGPT - restricted enterprise environment)
 - Address: 3180 18th Street, San Francisco, CA 94110, USA
 - Activities: Processing of text files for the purpose of translations and improving the quality of documentation. • Type of processing: Temporary processing of text that may contain personal data. Data is not used for model training.
 - International data transfer: Processing takes place on the basis of valid Standard Contractual Clauses and additional technical and organizational measures in accordance with Articles 44-49 GDPR.
3. Freeday B.V.
 - Address: Vijverhofstraat 47, 3032 SB, Rotterdam
 - Activities: Set-up, configuration, and maintenance of AI environments, workflows, and chatbot technology for Cloud86.
 - Type of processing: Access to systems and configurations in which personal data may be processed, for the purpose of optimizing, supporting, and developing AI functionality.

Annex 3: Technical and organisational measures

The technical and organizational measures taken by the contractor to ensure data protection and data security are described below. The aim is to guarantee, in particular, the confidentiality, integrity and availability of the personal data processed by the Contractor.

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

(1) Access

Measures to prevent unauthorised persons from gaining access to the data processing equipment used to process personal data.

- The data processing equipment, with the help of which the Client's data is processed, is located in separate locked rooms, to which only authorized persons have the right of access.
- Access to the data processing systems is secured by magnetic or chip cards. Access is logged.
- Exterior windows are secured by special protective measures.
- Rooms are secured by an alarm system.
- Access to the rooms is under video surveillance.

(2) Physical access control

Measures to prevent unauthorised persons from using the data processing equipment:

- The use of the data processing systems and programs is only possible by authorized users who have the appropriate access authorization.
- PCs are automatically locked if the user is inactive for a longer period of time.
- Authorized users are required to keep their access data secret and not to make them accessible to third parties.
- There are minimum standards for passwords. Passwords must also be changed regularly.

- For particularly sensitive data processing methods, registration using two-factor authentication is required.
- Data is deleted using secure deletion programs.

(3) Access control

Measures to ensure that those authorised to use the data processing procedures can only access the personal data subject to their access authorisation, as well as other measures to ensure the confidentiality of the systems and services:

- There are authorization concepts and needs-based access rights. To ensure exclusively authorized use, users have been set up with appropriate graduated access authorizations at program or folder level in the IT network.
- Access and file changes are logged. The protocols themselves are subject to regular checks.

(4) Separation control

Measures to ensure that personal data collected for different purposes can be processed separately from each other:

- The separation of the Client's data from its own data is carried out by logical separation of the data processing systems within the framework of the authorisation concept.

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

(1) Data processing control and transfer control, including control for the permanent integrity of systems and services

Measures to ensure that personal data are not stored, noted, modified, copied, deleted, removed, destroyed or otherwise processed without authorisation or accidentally, as well as measures to check and determine where the personal data is to be or have been transmitted by means of data transmission devices:

- In accordance with the performance of the tasks, graduated access authorizations are set up for the authorized employees at program or folder level in the IT network in order to prevent unauthorized reading, copying, modification, removal or transmission of the data during processing or use.
- Data is transmitted and transported electronically by means of secure processes. Data transmissions are logged.
- The existing security systems are regularly monitored. In the event of security messages, automatic escalation takes place.

- Removable storage devices are not used.
- Use of Virtual Private Networks (VPN) for external access to the company network.

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

(1) Availability check

Measures to protect against accidental or intentional destruction or loss of data:

- Backup-Strategie (online/offline; on-site/off-site)
- Uninterruptible power supply (UPS)
- A central firewall, which is supported by a virus scanner, protects the company network from unauthorized access from the outside and monitors the respective connection. PCs that have access to the outside (external media, Internet, e-mail) are also equipped with a local virus scanner.
- Data processing systems are subject to regular security updates.

(2) Rapid recoverability (Art. 32 para. 1 lit. c GDPR)

The ability to quickly restore the availability of and access to the personal data in the event of a physical or technical incident:

- Backup strategy (online/offline; on-site/off-site) (see above)

4. Procedures for regularly reviewing, assessing and evaluating the effectiveness of the technical and organisational measures to ensure the security of processing (Art. 32 para. 1 lit. d; Art. 25 para. 1, 2 GDPR)

Measures to review, evaluate and evaluate the effectiveness of these technical and organisational measures:

- The technical and organisational measures taken are regularly checked with regard to effectiveness and topicality.
- The regular review, evaluation and evaluation is recorded.
- In the event of security messages, an automatic escalation to the responsible employees takes place.

5. Privacy-friendly default settings (Art. 25 para. 2 GDPR)

Measures to ensure that, by default, only personal data whose processing is necessary for the specific purpose of processing is processed.

- Input masks are used to request only the data that is required for the respective processing purpose.
- Access to data according to the authorization concept.
- Limitation of the storage period by deletion concept.

6. Order control

No commissioned data processing within the meaning of Art. 28 GDPR without corresponding instructions from the client:

- Clear contract drafting
- Formalized order management
- Strict selection of the service provider
- Obligation to convince in advance

7. Organizational control

Measures to ensure that the or internal organisation meets the special requirements of data protection:

- All employees (including trainees and interns) and external service providers are obliged to comply with the data protection requirements under the GDPR as well as data secrecy according to § 53 BDSG.
- Employees are regularly trained in data protection law to the extent necessary.

Annex 4: Persons authorised to issue instructions

The following persons are authorised to issue and receive instructions:

I. At the client's premises:

Name	Telephone number	E-mail address

II. At the contractor:

Name	Telephone number	E-mail address
Maurice Graber	+31 85 7991 000	info@cloud86.io