DATA PROCESSING AGREEMENT

The undersigned:

1. Snakeware New Media B.V., established in Sneek and with its principal place of business at Veemarktplein 1, 8601DA in Sneek, duly represented in this matter by H.A. Hoomans, CEO, hereinafter to be referred to as: the "***Processor***",

2. Name of client, hereby legally represented by its director who is authorized to sign, hereinafter to be referred to as: the "***Controller***",

Hereinafter also jointly referred to as: the "***Parties***",

Declare that they have agreed as follows:

Clause 1 Definitions

1. Agreement: The agreement concluded between the Parties on [*date*] concerning the digital productions delivered by the Processor to the Controller, and for which the Processor processes personal data on behalf of the Controller.
2. Data Processing Agreement: this agreement which forms an inseparable part of the Agreement, which executes Article 28 (3) of the GDPR.
3. GDPR: Regulation 2016/697, the General Data Protection Regulation.
4. EEA: the European Economic Area.
5. Personal Data Breach: a breach of security involving personal data, as meant in Article 4 (12) of the GDPR.
6. Subprocessor: 'another processor' engaged by the Processor as meant in Article 28 (2) and (4) of the GDPR.
7. In case definitions are used which correspond to definitions in the GDPR, these definitions have the same meaning as in the GDPR.
8. The Controller is deemed to be the controller as meant in Article 4 (7) of the GDPR.
9. The Processor is deemed to be the processor as meant in Article 4 (8) of the GDPR.

Clause 2 Subject of this Processing Agreement

1. The Controller is responsible for processing the personal data within the context of the performance of the Agreement. The Processor does not have independent control over the Personal Data.
2. The Processor processes personal data solely on the instructions of the Controller and to the extent necessary within the context of performing the Agreement, in accordance with the purposes and means determined by the Controller and categories of personal data and data subjects stated in **Annex 1**, as well as in accordance with any other written instructions issued by the Controller, unless a provision under Union or Member State law to which the Processor is subject provides that the Processor is obliged to process personal data, in which case the Processor will notify the Controller of that statutory provision before the Processing takes place, unless that legislation prohibits such notification on important grounds of public interest.

3. The Controller warrants that the content, use and instruction to process personal data as meant in this Data Processing Agreement are not unlawful and do not violate any third party rights. The Controller indemnifies the Processor for all claims related thereto.
4. The Processor informs the Controller without undue delay if, in its opinion, instructions conflict with the GDPR or are otherwise unreasonable.
5. This processor agreement, once signed by the Parties, shall form an integral and inseparable part of the Agreement.

Clause 3 Technical and organisational security measures

1. The Processor shall, having regard to the state of the art and the costs of implementation, also taking into account the provisions of Article 32 GDPR, undertake best efforts to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. These measures may change from time to time. Controller waives – given the (scalable) nature of the Services – the right to give specific instructions to the Processor regarding the security measures. An overview of the most recent security measures is available on request at the Processor.
2. The Controller will only provide the Processor with personal data for processing if the Controller has assured itself that the requisite security measures are appropriate and adequate.
3. If the Processor becomes aware of Personal Data Breach, the Processor will inform the Controller about this without undue delay after the Processor has become aware of the Personal Data Breach. The Controller is at all times responsible for notifying the Personal Data Breach with the supervisory authority and, in case of a high risk, to the data subject(s).
4. If a Personal Data Breach occurs, despite the Processor having implemented the measures as agreed with the Controller, the Controller may not hold the Processor liable for any damage incurred by the Controller as a result.

Clause 4 Engaging Subprocessors

1. The Processor may outsource the obligations pursuant to the Agreement to Subprocessors. The most recent overview of Subprocessors is available at the Processor on the Controller's request.
2. The Processor will not engage new Subprocessors without informing the Controller in a timely manner. The Controller has the right to object to any new or changes Subprocessor, in writing and within one (1) week after the Processor has sent notification of this, with a reasoned objection. If the Controller objects, the Parties will consult each other to reach a solution.
3. The Processor will oblige any Subprocessors to comply with materially similar provisions included in this Data Processing Agreement. The Processor will at all times be responsible for the acts or omissions of the Subprocessors.

Clause 5 Transfers to third countries

1. The Processor is allowed to process the personal data in countries within the EEA. Additionally, the Processor may process personal data in countries outside the EEA, if such transfer is in line with Chapter V of the GDPR, for example of the receiving country has received an adequacy decision from the European Commission, or if the Processor concludes Standard Contractual Clauses with the receiving party.
2. The most recent overview of processing locations is available at the Processor on the Controller's request.

Clause 6 Providing assistance

1. Taking into account the nature of the Processing, the Processor will cooperate fully with the Controller by means of appropriate technical and organisational measures, insofar as is possible, to the extent necessary for the Controller to satisfy requests from data subjects whose personal data are being processed as referred to in Chapter III of the GDPR.
2. Taking into account the nature of the Processing and the information that is at its disposal, the Processor will provide the Controller with assistance in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR.
3. The Processor may charge reasonable costs to the Controller for providing assistance based on this Clause.
4. A complaint received by Processor or a request for inspection regarding the processing of Personal Data shall be forwarded by Processor to Controller without delay.

Clause 7 Confidentiality

1. The Processor, as well as all of its employees who have access to the personal data, are obliged to maintain secrecy with regard to the personal data to which they have access.
2. This duty of confidentiality does not apply insofar as the Controller has given permission to provide the personal data to third parties, if the provision of personal data to third parties is logically necessary in view of the nature of the instruction provided and the execution of this Data Processing Agreement, or if there is a statutory obligation to provide the information to a third party.

Clause 8 Disclosure & deletion

Upon termination of the Agreement, the Processor will, at the Controller's discretion, delete all personal data or return all Personal Data to the Controller in a common format and will delete existing copies, unless the personal data must be stored pursuant to applicable legislation.

Clause 9 Liability

1. If the Processor is liable to the Controller for any loss from whatever cause, without prejudice to the provisions of clause 3 (4), the Processor will only be liable for direct loss suffered by the Controller as a result of an attributable failure by the Processor and/or an unlawful act. The total liability under the Agreement, including the Data Processing Agreement or any violation by the Processor and/or Subprocessors of the applicable national or EU privacy regulations, will never amount to more than the maximum amount actually paid by the cyber insurance of Processor.
2. The Processor will never be liable for consequential loss, including purely financial loss, loss of profits and immaterial loss. In particular, the Processor is never liable for loss in connection with or as a result of:
    a. termination or change to the service provided;
    b. failure to communicate about problems with hardware, software, the network or other computer-related problems
    c. the use of data or data files in accordance with the Controller's instructions
    d. loss, corruption or destruction of data or data files; and/or
    e. the Processor's service not being accessible.
3. To the extent that compliance is not permanently impossible, the Processor is only liable for attributable failure to fulfil the Data Processing Agreement if the Controller properly and without delay

declares in writing that the Processor is in default, providing a reasonable term to remedy the failure and the Processor continues to be in default after this term. The notice of default must include a description of the failure that is as complete and detailed as possible so as to allow the Processor to respond adequately.

4. In any case, any right to compensation is only acquired if the Controller notifies the Processor in writing of the damage as soon as possible. Any claim for damages against the Processor will lapse solely by the expiry of six (6) months after the claim arises.
5. To the extent that the Processor Parties are jointly and severally liable towards third parties, including the data subject, or are jointly fined by the Personal Data Authority, the Parties shall be obliged towards each other, each for the part of the debt that concerns him in their mutual relationship, to contribute to the debt and costs in accordance with the provisions of Book 6, Title 1, Section 2 of the Dutch Civil Code, unless the GDPR provides otherwise in which case the GDPR takes precedence.

Clause 10 Costs

1. Data processing costs inherent in the normal performance of the Agreement shall be deemed to be embedded in the fees already due under the Agreement.
2. Any support or any other additional services to be provided by Processor under this Processor Agreement, or requested by Processor, including any requests for additional information, will be charged to Processor.

Clause 11 Audit

1. The Controller may, at its own expense, verify the Processor's compliance with this Data Processing Agreement by having an audit performed by an independent third party which is approved by the Processor, provided that the Controller informs the Processor of this at least ten (10) working days in advance and provided that during the audit, the Controller follows the Processor's reasonable instructions and the audit does not present an unreasonable disruption to the Processor's business operations.
2. The audit may be performed once a year maximum or more in case of a reasonable suspicion of non-compliance with this Data Processing Agreement by the Processor, which has been communicated in writing and approved by the Processor.
3. The audit and its results will be integrally shared by Controller with Processor as soon as possible handled as confidential information by the Controller.

Clause 12 Rights of third parties

This Processor Agreement does not and does not grant any rights or benefits to any person, now or in the future, who is not a Party to this Processor Agreement.

Clause 13 Miscellaneous

1. If one or more provisions of this Data Processing Agreement conflict with one or more provisions of other agreements between the Controller and the Processor, this Data Processing Agreement will prevail.
2. This Processor Agreement has a term equal to the Agreement (including any extension thereof) and cannot be terminated prematurely.
3. Processor is entitled to suspend the performance of this Processor Agreement and the related Agreement, or to terminate them without judicial intervention, if the Processor:

(a.) is dissolved or otherwise ceases to exist;
b.) fails to fulfil its obligations under this Processor Agreement and that attributable failure has not been remedied within 30 days after written notice of default to that effect;
c.) is declared bankrupt or applies for a moratorium.

4. If any provision of this Data Processing Agreement is declared void or is nullified, or if it is necessary to amend this Data Processing Agreement or one of its provisions in order to comply with the applicable privacy laws and regulations, the other provisions will remain in full force. The Parties will then either draw up a new provision to replace the void/nullified provision or amend this Data Processing Agreement to bring it into line with the applicable privacy laws and regulations, duly observing the purport of the void/nullified provision to the extent possible.
5. This Data Processing Agreement is governed by Dutch law.
6. Any and all disputes between the Controller and the Processor will be submitted solely to the court which is competent based on the Agreement.

Signatures

Place and date	Place and date
Controller	Processor

Annex 1

Specification of services, purposes and personal data
All options are listed in the following annexes. However, only the options that relate to your specific situation are applicable.

1A Services
Processor processes personal data in the context of (one or more of) the following services:
Snakeware CMS software (Snakeware.cloud, CMS Enterprise)
Web hosting
Backup
Load balancing/failover
SSL certificates
Invoicing
Transfer of defaulters' data to various institutions

1B Purposes
Processor processes personal data for (one or more of) the following purposes:
Content management software
Hosting, cloud storage
Security
Network set-up
Customer information for billing purposes

1C Categories
Processor processes (one or more of) the following categories of personal data on behalf of Processor:

Name and address details
Contact details
Identification number
Customer number
Payment details
Resume
Date of birth
Gender
Marital status
Nationality
Login details
Financial and payment details
IP address
Social media accounts
Data on click and surfing behaviour
Data on orders and use of services/products
Contents of emails, contact forms, instant messages and other communications
Registration number

Location data
Passport photos
Camera images
Personnel file
Biometric data
Citizen service number (BSN)
Genetic data
Copy of ID card
Belief or religion Race
Sexual preference
Trade union membership
Health data/medical data
Criminal data or data relating to unlawful/harassing behaviour
Other data stored or otherwise to be processed through Processor's services

1D Data subjects
This concerns one or more of the following categories of data subjects:

Customers
Website visitors
Employees
Applicants
Account holders
Potential customers
Suppliers
CMS Editors
Other categories of persons whose personal data are processed through the services of Processor

Controller warrants that the personal data and categories described in Annex 1 are complete and correct, and indemnifies Processor against any defects and claims resulting from an incorrect representation by Controller.

Annex 2: Security measures

1) Security Measures. Processor shall implement and maintain security measures applicable for monitoring User Data against accidental or unlawful destruction, loss, alteration, disclosure or access (collectively referred to as "Security Measures"). The security measures are based on the state of the art and what is feasible within realistic budgets, applied to the nature, scope and objectives of the data processing, as well as the budgeted risks and severity of any breach of user rights.

Security measures include, where applicable, (1) anonymizing and/or encrypting personal data, (2) the ability to ensure the confidentiality, integrity, availability and robustness of data processing and services, (3) the ability to ensure the availability and accessibility of personal data in the event of an incident, and (4) a process for periodically testing and evaluating the effectiveness of technical and organizational measures for monitoring the security of our data processing.

Processor may adjust the security measures around data processing at any time, with the understanding that such adjustments will not reduce the security of its services.

2) Security measures around employees. Processor shall take precautions to ensure that employees, employees on a temporary basis and data processors comply with security measures within the scope of their work for Processor, as well as strict confidentiality for all concerned regarding data and work.

3) Within the agreement between Controller and Processor, the Enterprise Content Management Platform 'CMS Enterprise' or 'Snakeware.Cloud' (hereinafter referred to as CMS) is provided as a tool to the Controller, for the purpose of managing web applications and similar techniques (hereinafter referred to as sites). The CMS is a Software-As-A-Service (SaaS) product and the right to use the CMS is linked to ongoing maintenance/service contracts (SLA).

4) The CMS is used by Processor for the management of its sites, which has the effect that the information posted by Processor and any data posted by third parties can be displayed and edited via the CMS for editorial purposes.

5) All information displayed and edited through the CMS will be stored in the database belonging to the Controller's site. In part, this information will be temporarily stored in the memory of the CMS server for the purpose of improving the user experience (primarily this is caching frequently used data for speed).

7) A limited set of user data of the editors using the CMS for managing the Processor's sites will be stored by Snakeware.