DATA PROCESSING AGREEMENT (ART 28 GDPR) FOR STREAMDIVER CLOUD SERVICES

("AGREEMENT" OR "DPA")

This Data Processing Agreement is included in agreements between Streamdiver GmbH (hereinafter referred to as "SD") and third parties ("Client") regarding the provision of cloud services including support and governs the processing of Personal Data by SD on behalf of the Client in this relationship.

1 DEFINITIONS

Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, whether directly as a processor of a controller or indirectly as a sub-processor of a processor who processes personal data on behalf of the controller.
Client data	means all content, materials, data, personal data and information collected, processed and managed by Authorized Users in the production system of a Cloud Service.
Authorized user	(or "Named User") means a person who works at the Client's company or at business partners of the Client and to whom the Client has granted access authorization for the Cloud Service.
Order	or "Agreement" means an agreement between SD and the Client on the basis of an offer made by SD and an acceptance of the offer for Cloud Services which is consistent with the content of the offer and which refers to the Terms of Use (and any other documents).
Person concerned	means an identified or identifiable natural person as defined in data protection law.
Cloud service	means any specific on-demand solution (including support) provided by SD under a Purchase Order.
Data protection law	means the applicable legislation protecting the fundamental rights and freedoms of individuals and their right to privacy in relation to the processing of Personal Data under the Agreement (and includes, in relation to the relationship between the parties regarding the processing of Personal Data by SD on behalf of the Client, the GDPR as a minimum standard, regardless of whether the Personal Data is subject to the GDPR or not).
EU standard contractual clauses	(also referred to as the "EU Model Clauses") means the Standard Contractual Clauses (Processors) or any subsequent versions of these clauses published by the European Commission (which apply automatically).
EEA	refers to the European Economic Area, i.e. the member states of the EU plus Iceland, Liechtenstein and Norway.
Personal data	means any information relating to a Data Subject that is subject to the protection of data protection law. In this DPA, it means only that personal data which (i) is collected by the Customer or its Authorized Users in or through the use of the Cloud Service or (ii) is provided by SD or its sub-processors or accessed by SD or its sub-processors in order to provide support under the Agreement. Personal Data is a subset of the Customer Data.
Sub-processors	means affiliated companies of SD and third parties that are used by SD to provide the Cloud Service and that process Personal Data in accordance with this DPA.
Person responsible	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where the SD Client acts as a processor for another controller, the Controller shall be deemed to be an additional and independent controller with the corresponding rights and obligations of a controller under this DPA.

2 SUBJECT MATTER OF THE AGREEMENT

2.1 The object of the order placed with SD is the provision of IT services on the basis of and within the scope of the order.

2.2 SDs and clients are each responsible for checking and implementing the requirements placed on controllers and processors under applicable data protection law.

2.3 SD will act as a processor and the Client, or the legal entities that the Client authorizes to use the Cloud Service, will act as controllers under the DPA. The Client is the sole point of contact and solely responsible for obtaining all relevant authorizations, consents and approvals for the processing of Personal Data under this DPA. To the extent that authorizations, consents, instructions or consents are granted by the Client, they are granted not only on behalf of the Client, but also on behalf of any other controllers using the Cloud Service. If SD informs or notifies the Principal, such information or notifications shall be deemed to have been received from those controllers to whom the Principal has authorized the use of the Cloud Service. It is the responsibility of the Principal to forward this information and notifications to the relevant responsible parties.

2.4 Each Party shall be responsible for complying with its documentation obligations, in particular for keeping records of processing activities to the extent required under Data Protection Law. Each Party shall reasonably assist the other Party in fulfilling its documentation obligations, including providing the other Party with the information it requires in a form reasonably requested by the other Party to enable the other Party to comply with the obligations relating to the maintenance of processing records.

3 PROCESSING TO ORDER

3.1 As part of the provision of the Cloud Service, SD usually processes data of the following categories:

3.1.1. Name / Username

3.1.2. E-mail address

3.1.3. IP address

3.1.4. Rights & roles - Group membership/system access/usage and authorization data

3.2 Affected persons are authorized users and therefore typically employees or business partners who are granted access to the cloud service by the client.

3.3 The personal data is essentially subjected to the following processing measures:

3.3.1. Use of Personal Data to set up, operate, monitor and provide the Cloud Service (including operational and technical support)

3.3.2. Provision of consulting services

3.3.3. Communication with authorized users

3.3.4. Storage of personal data in special data centers (multi-tenant architecture)

3.3.5. Upload corrections or upgrades to the cloud service

3.3.6. Creating backup copies of personal data

3.3.7. Computerized processing of personal data, including data transmission, retrieval of data, access to data

3.3.8. Network access to enable the transfer of personal data

3.3.9. Execution of the client's instructions in accordance with the agreement

4 OBLIGATIONS OF THE PROCESSOR

4.1 SD will only process Personal Data in accordance with the Client's documented instructions. The Agreement (including this DPA) constitutes such documented initial instruction and each use of the Cloud Service constitutes a further instruction. SD shall make all reasonable efforts to comply with all other instructions of the Client to the extent required by data protection law, technically feasible and possible without changes to the Cloud Service. If one of the aforementioned exceptions applies or SD is otherwise unable to comply with an instruction or believes that an instruction violates data protection law, SD will notify the client immediately (e-mail permitted).

4.2 SD may also process Personal Data where required by applicable law. In such a case, SD will inform the Client of these legal requirements prior to processing, unless the relevant regulation prohibits such information.

4.3 SD and any sub-processors shall only grant access to the processing of Personal Data to authorized persons who have committed themselves to confidentiality. SD and sub-processors will regularly train the persons who have access to Personal Data with regard to the applicable data security and data protection measures.

4.4 At the Principal's request, SD will reasonably cooperate with the Principal to deal with any requests from Data Subjects or supervisory authorities regarding SD's processing of Personal Data. SD will inform the Principal as soon as reasonably possible of any request received by SD from a Data Subject in connection with the processing of Personal Data, without itself responding to such request without further instructions from the Principal. SD will provide functionality to support the Client's ability to rectify or erase Personal Data from the Cloud Service or to restrict processing in accordance with Data Protection Law. If such functionality is not provided, SD will rectify or erase or restrict the processing of Personal Data in accordance with the Client's instructions and Data Protection Law.

4.5 SD will notify Customer of a Personal Data Breach without undue delay after becoming aware of it and provide Customer with adequate information available to SD to assist Customer in fulfilling its obligations to notify a Personal Data Breach in accordance with the requirements of Data Protection Law. SD may provide this information in sections as and when it becomes available. Such notification is not an admission of fault or liability on the part of SD and shall in no way be construed as such.

4.6 If the Principal (or its controllers) are required under data protection law to carry out a data protection impact assessment or prior consultation with a supervisory authority, SD will provide those documents that are generally available for the Cloud Service (e.g. this DPA, the Agreement or any audit reports or certifications) at the Principal's request. Any additional support shall be mutually agreed between the Parties.

5 DATA SECURITY

5.1 SD declares in a legally binding manner that all appropriate and necessary measures have been taken to ensure the security of the processing in accordance with Art 32 GDPR, taking into account the state of the art, the implementation costs, the nature, scope, context and purposes of the processing of Personal Data. SD has implemented and will apply the technical and organizational measures listed in Annex 1 for this purpose.

5.2 Changes. SD applies the technical and organizational measures described in Annex 1 equally to all SD Customers (except for the options listed in Section 9) hosted in the same data center and receiving the same cloud service. SD may change the measures listed in Appendix 1 at any time without notice as long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without compromising the security level for the protection of Personal Data.

6 DATA EXPORT & DATA DELETION

6.1 Export and removal by the client: During the term and in accordance with the provisions of the agreement, the client may access its personal data at any time. The Client may extract its Personal Data and export it in a standard format. Retrieval and export may be subject to technical restrictions and requirements. In this case, SD and Principal shall agree on an appropriate method to enable Principal's access to the Personal Data.

6.2 Deletion. Prior to the end of the Contract, the Client may use SD's available self-service export tools to perform a final export of the Personal Data from the Cloud Service (which corresponds to a return of the Personal Data). The Principal hereby instructs SD to delete the Personal Data remaining on the servers used to host the Cloud Service within a reasonable time after the end of the contract in accordance with data protection law (at the latest within 6 months), unless their retention is required under applicable law.

7 SUBPROCESSORS

7.1 SD is hereby authorized in writing to transfer the processing of Personal Data to sub-processors under the following conditions:

7.1.1. SD shall inform the client of the identity and role of the sub-processor prior to the conclusion of the contract, unless the use of the sub-processor is only necessary due to the specific requirements and specifications of the client;

7.1.2. SD shall engage sub-processors under written contracts (including in electronic form) that comply with the provisions of this DPA in relation to the processing of Personal Data by the sub-processor. SD shall be liable for any breaches by the sub-processor in accordance with the terms of this Agreement;

7.1.3. SD will assess the security, privacy and confidentiality practices of a sub-processor before selecting it to determine that it is capable of providing the level of protection for Personal Data required by this DPA.

7.2 The use of new sub-processors is subject to compliance with the following regulations:

7.2.1. SD will inform the Client in advance (by email or through a notification within the Cloud Service) of any planned additions or replacements within the list of approved Sub-Processors, including the name, address and role of the new Sub-Processor; and

7.2.2. the client may object to such changes in accordance with the following section.

7.3 Objection to new sub-processors.

7.3.1. If the Principal has a legitimate reason under data protection law to object to the processing of Personal Data by the new sub-processors and SD uses the sub-processor despite the Principal's objection, the Principal may terminate the Agreement (limited to the service part for which the new sub-processor is to be used) by written notice to SD with effect from a date specified by the Principal, but no later than the expiry of thirty days after the date of SD's notification to the Principal of the new sub-processor. If the Principal does not terminate within this period of thirty days, the new sub-processor shall be deemed to have been approved by the Principal.

7.3.2. Within the thirty day period from the date of SD's notice to the Client informing the Client of the new Subprocessor, the Client may request that the parties meet in good faith to discuss a resolution of the objection. Such discussions shall not extend the notice period and shall not affect SD's right to engage the new sub-processor(s) after the expiry of the thirty day period.

7.3.3. Any termination under this Section 7.3 shall be deemed by both parties to be without fault and subject to the terms of the Agreement.

7.4 Emergency replacement: SD may replace or appoint a Sub-Processor without prior notice if the reason for the appointment/replacement is beyond SD's reasonable control and the immediate replacement is necessary for security or other urgent reasons. In this case, SD will inform the Principal of the new sub-processor immediately after its appointment. Section 7.3 applies accordingly.

8 INTERNATIONAL PROCESSING

8.1 SD is entitled to carry out the processing of Personal Data with the involvement of sub-processors within the meaning of this DPA outside the country in which the client is located, in compliance with data protection law.

8.2 As a matter of principle, SD only uses sub-processors based within the European Union.

8.3 Without the express consent of the client, SD will not transfer any personal data of the client to sub-processors based in the USA, as it can currently be assumed that it is not possible to guarantee an adequate level of data protection in the USA even by using standard contractual clauses.

8.4 If (i) personal data of a controller established in the EEA or Switzerland are processed in a country outside the EEA, Switzerland or outside a country, organization or territory recognized by the European Union as a safe country with an adequate level of data protection pursuant to Art. 45 GDPR, or (ii) Personal Data of another controller is processed internationally and such international processing requires an adequate means under the applicable law of the controller, and the adequate means can be fulfilled by entering into standard contractual clauses, SD shall ensure that any such processing is based on the EU standard contractual clauses. Otherwise, no international processing will take place.

ANNEX 1

Technical and organizational measures

The following sections define SD's current technical and organizational measures. SD may change these measures at any time without notice as long as a comparable or higher level of security is maintained or achieved. Individual measures may be replaced by new measures that fulfill the same purpose without reducing the security level for the protection of Personal Data.

1 Access control

1.1 Unauthorized persons are denied physical access to facilities, buildings and premises in which data processing systems that process or use personal data are located.

1.2 Measures:

- SD protects buildings through appropriate measures based on the SD Security Policy.
- In general, buildings are secured by access control systems (e.g. access by chip card).
- As a minimum requirement, the external entrances to a building must be equipped with a certified locking system, including a modern, active key management system.
- Depending on the security classification, buildings, individual areas and the surrounding grounds may be protected by additional measures. These include special access profiles, video surveillance, intruder alarm systems and biometric access control systems.
- Access rights are assigned to authorized persons on an individual basis in accordance with the measures for system and data access control (see sections 1.2 and 1.3 below). This also applies to the access of visitors. Guests and visitors in SD buildings must register by name at the reception desk and be accompanied by authorized SD personnel.
- Additional measures for data centers:
    - Biometric access control system (using fingerprints)
    - Contactless key card
    - Separation system
    - Individually locked server cabinets (documented key allocation)
    - Security zones and spatial separation (data center > room > cage in room > server cabinet)
    - 24/7 video surveillance
    - 24/7 security personnel in the data center
    - ISO27001 certification
    - ISO9001 certification

2 System access control

2.1 Data processing systems used to provide the Cloud Service must be protected against unauthorized use.

2.2 Measures:

- Access to sensitive systems, including systems for storing and processing personal data, is granted via several authorization levels.
- Authorizations are managed via defined processes in accordance with the SD Security Policy.
- All persons access SD's systems with a unique identifier (user ID)
- SD has established procedures so that requested changes to authorizations are only made in accordance with the SD Security Policy (for example, no rights are granted without appropriate authorization). When an employee leaves the company, their access rights are revoked.
- SD has established a password policy that prohibits the disclosure of passwords, regulates how to proceed if a password is disclosed and requires passwords to be changed regularly and default passwords to be changed. Personalized user IDs are assigned for authentication purposes. All passwords must meet certain minimum requirements and are stored in encrypted form. In the case of domain passwords, the system enforces a password change every six months, which must meet the requirements for complex passwords. Each computer has a password-protected screen saver.
- The company network is protected from the public network by firewalls.
- SD uses up-to-date virus scanners at the transitions to the company network (for e-mail accounts), as well as on all file servers and on all standalone computers.

- Security patch management ensures the application of appropriate regular security updates. Full access to the SD corporate network and critical infrastructure is protected by strict authentication.

3 Data access control

3.1 Persons who are authorized to use data processing systems are only granted access to the personal data for which they have access rights, and personal data may not be read, copied, modified or removed without authorization during processing, use or storage.

3.2 Measures:

- In the context of the SD Security Policy, personal data requires at least the same protection as "confidential" information in the sense of the SD Information Classification Standard.
- Access to personal data is only granted when necessary ("need-to-know" principle). Each person is only granted access to the information they need to perform their duties. SD uses authorization concepts that document the assignment processes and the roles assigned per account (user ID). All client data is protected in accordance with the SD Security Policy.
- All productive servers are operated in data centers or in secure server rooms. The security measures to protect the applications for processing personal data are checked at regular intervals. To this end, SD conducts internal and external security audits and penetration tests of its IT systems.
- SD does not permit the installation of proprietary software or other software that has not been authorized by SD.
- A corresponding SD security standard regulates how data and data carriers are deleted or destroyed when they are no longer required.

4 Data transfer control

4.1 Data transmission control ensures that Personal Data cannot be read, copied, modified or removed without authorization during transmission or storage, except to the extent necessary for the provision of the Cloud Services in accordance with the Agreement. During the physical transportation of data media, SD will take appropriate measures to ensure the agreed service levels (e.g. encryption, lead-lined containers).

4.2 Measures:

- Personal data is protected during transmission via internal SD networks in accordance with the SD Security Policy.
- With regard to the transfer of data between SD and its clients, the security measures for the transferred personal data are agreed by the parties and form part of the agreement. This applies to both physical and network-based data transmission. In any case, the Principal assumes responsibility for the data transfer once it takes place outside the systems controlled by SD (e.g. data transferred outside the firewall of the SD data center).

5 Data entry control

5.1 It will be possible to retrospectively investigate and determine whether and by whom personal data was collected, modified or removed from the data processing systems of the SD.

5.2 Measures:

- SD only allows authorized persons to access personal data within the scope of their duties.
- SD has implemented a logging system within the Cloud Service for the collection, modification and deletion or blocking of Personal Data by SD or its sub-processors to the extent technically possible.

6 Order control

6.1 Personal data processed on behalf of the client (e.g. on behalf of the client) will only be processed in accordance with the agreement and the client's instructions in this regard.

6.2 Measures:

- SD uses controls and procedures to monitor compliance with contracts between SD and its clients, sub-processors or other service providers.
- In the context of the SD Security Policy, personal data requires at least the same protection as "confidential" information in the sense of the SD Information Classification Standard.
- All SD employees and sub-processors or other service providers will be contractually bound to maintain confidentiality with respect to all sensitive information, including trade secrets, of SD's clients and partners.

7 Availability control

7.1 Personal data is protected against accidental or unauthorized destruction or loss.

7.2 Measures:

- SD has regular backup processes to restore the availability of business-critical systems if required.

- SD uses uninterruptible power supplies (UPS, batteries, generators, etc.) to protect the power supply for the data centers.
- SD has developed business contingency plans for business critical processes and can provide disaster recovery strategies for business critical services as detailed in the documentation or included in the order for the relevant cloud service.
- Emergency processes and systems are tested regularly.

8 Separation control

8.1 Personal data collected for different purposes can be processed separately.

8.2 Measures:

- SD uses the technical possibilities of the implemented software (e.g. multi-tenancy or separate system landscapes) to enable the separation of personal data originating from different clients.
- The client (including those responsible) only has access to its own data.
- If personal data of the client is required to process a support case of the client, the data is assigned to this message and only used to process this message; this data is not accessed for processing other messages. This data is stored in dedicated support systems.

9 Data integrity check

9.1 Personal data remains intact, complete and up-to-date during processing activities.

9.2 Measures:

SD has implemented a multi-layered security strategy to protect against unauthorized changes. In particular, SD uses the following means to implement the above sections on controls and measures:

- Firewalls
- Security monitoring
- Antivirus software
- Creating backup copies and restoring
- External and internal penetration tests
- Regular inspection of security measures by external auditors