Data Processing Agreement

Parties:

1. Customer as "Controller"
2. DataSnipper as "Processor"

hereinafter jointly referred to as: "**Parties**" and separately as "**Party**";

taking into consideration that:

A. this Data Processing Agreement ("DPA") is entered into in connection with the licensing of the DataSnipper Software by the Processor to the Controller and governs the execution of the contract between DataSnipper and the Customer ("Contract");
B. the Processor shall process personal data as defined by applicable data protection laws, including but not limited to the General Data Protection Regulation ("GDPR"), the UK GDPR, the California Consumer Privacy Act (CCPA) and other relevant data protection regulations (collectively referred to as 'Applicable Data Protection Laws');
C. any definitions used that correspond to the definitions set out in the GDPR have the same meaning;
D. Parties, also in view of the requirement of Article 28 (3) of the GDPR, wish to lay down their rights and obligations in writing by means of this DPA.

have agreed the following:

1 Scope and purpose of processing

1.1 Processor undertakes to process personal data on behalf of the Controller according to the provisions laid down in this DPA. Data processing shall take place in the context of the execution of the Contract, as well as those purposes that are reasonably related to it or that are determined in Contract.

1.2 The data processing relates to the data processing purposes set by the Controller regarding the categories of personal data and data subjects listed in **Appendix A** to this DPA. Processor shall not make any independent decisions regarding the processing of personal data for other purposes.

1.3 Due to the nature of Processor's services, Processor has no visibility or insight into, nor any control over, whether the documents uploaded by the Controller to the Processor's platform and/or functionalities contain personal data, nor over the nature or categories of such personal data. Accordingly, the provisions of the Data Processing Agreement shall apply insofar as and to the extent that the Controller, in the course of using the Processor's services, processes documents or data containing personal data. By using Processor's services, the Controller thereby instructs Processor to process all personal data contained in the data or documents uploaded by the Controller to Processor services.

1.4 The personal data to be processed on the instructions of Controller will remain the property Controller and/or the data subjects involved.

2 Obligations Processor

2.1 With regard to the data processing activities referred to in Article 1, the Processor shall comply with the Applicable Data Protection Law.

2.2 Processor shall inform the Controller of the measures it has taken with respect to its obligations under this DPA when this is first requested by the Controller.

2.3 The obligations of the Processor ensuing from this DPA also apply to those who process personal data under the authority of the Processor, including but not limited to employees, in its broadest sense.

2.4 Processor shall immediately notify the Controller if it deems that data processing instructions are not in accordance with the Applicable Data Protection Law.

2.5 Processor shall assist the Controller in the fulfilment of its legal obligations. This concerns providing assistance in fulfilling its obligations under the Applicable Data Protection Law, such as providing assistance in carrying out a Data Protection Impact Assessment (DPIA) and prior consultation in the event of high-risk data processing.

3 Obligations of Controller

3.1 The Controller shall:

3.1.1 ensure that the Processing of Personal Data complies with the Applicable Data Protection Law;

3.1.2 ensure that Personal Data shall not contain any special categories of personal data as specified in article 9 GDPR or other types of sensitive personal data;

3.1.3 be responsible for providing the necessary notices to Data Subjects and obtaining any required consents for the Processing of Personal Data;

3.1.4 ensure that a record of Processing activities under its responsibility, if required under the Applicable Data Protection Law, is maintained;

3.1.5 appoint a data protection officer, if required under the Applicable Data Protection Law, and communicate their contact details to Processor;

3.1.6 cooperate with the supervisory authority as needed and inform Processor of any relevant correspondence with the supervisory authority that may impact Processor's obligations.

4 Transfer of personal data

4.1 Processor may process personal data in countries within the European Economic Area (EEA). In addition, Processor may also process the personal data to a country outside the EEA, provided that the country ensures an adequate level of protection and it complies with the other obligations incumbent on it under this DPA and the Applicable Data Protection Law.

5 Division of responsibility

5.1 Processor is solely responsible for the processing of the personal data under this DPA, in accordance with the instructions of Controller and under the explicit (final) responsibility of the Controller.

5.2 The Processor guarantees that the content, use and instruction of the processing of the personal data referred to in this DPA are not unlawful and do not infringe any third-party right.

6 Engaging sub-processors

6.1 Controller hereby authorises Processor to use third parties and Affliates (sub-processors) when processing personal data, pursuant to this DPA, in compliance with the Applicable Data Protection Law.

6.2 An up-to-date list of sub-processors is published by Processor at https://www.datasnipper.com/legal/sub-processors. Controller may opt in to receive notifications of changes to this list by emailing legal@datasnipper.com. Absent such subscription, Controller acknowledges that publication on this webpage constitutes adequate notice of sub-processor changes.

6.3 The Controller has the right to object in writing, stating reasons, to any additional sub-processors engaged by Processor after execution of this agreement. Such objection must be submitted within fourteen (14) days from the date of notification. If Controller objects to any sub-processors engaged by the Processor, the Parties will consult with each other to find a solution. If the Parties are unable to resolve the objection within a reasonable time period, which shall not exceed thirty (30) days, either Party may terminate the Agreement by providing written notice to the other Party.

6.4 Processor shall impose on the sub-processors engaged by it similar or more stringent obligations as agreed between the Controller and the Processor. Processor shall be responsible for the correct observance of these obligations by sub-processors and shall be liable for any damage caused by errors on the part of these sub-processors.'

7 Security

7.1 Processor shall take appropriate technical and organizational measures to protect the personal data processed on behalf of the Controller against loss or against any form of unlawful processing (such as unauthorised access, alteration, modification or disclosure of the personal data). A description of the technical and organizational measures implemented by the Processor is set out in **Appendix C**.

7.2 Processor does not guarantee that the security measures are effective under all circumstances. The Processor shall have the security meet a level that is not unreasonable in view of the technological state of the art, the sensitivity of the personal data and the costs associated with the implementation of the security measures.

7.3 DataSnipper is subject to periodic audits by a qualified and independent third-party auditor to assess and confirm its compliance with the security controls and procedures described in its applicable SOC 2 report.

8 Data breach notification obligation

8.1 Processor shall, without undue delay and, where feasible, no later than 72 hours after having become aware of a personal data breach (Hereafter: "Data Breach"), notify the Controller of a Data Breach.

8.2 The obligation to notify applies regardless of the impact of the Data Breach. The notification shall include at minimum the information listed in **Appendix B**. The Processor shall report the Data Breach by e-mail to the contact person listed in **Appendix B**.

8.3 The Data Processor shall follow all instructions of the Controller and provide the cooperation necessary to eliminate the cause of the Data Breach, to prevent further damage to the data subject(s) and to prevent similar incidents in the future.

8.4 The Processor shall document all data breaches, including the facts about the personal data breach, its consequences and the corrective measures taken.

9 Rights of data subjects

9.1 Should a data subject submit a request to the Processor to exercise their legal rights under Applicable Data Protection Law, the Processor shall immediately forward the request to the Controller and inform the data subject accordingly. The Controller shall then handle the request independently.

9.2 Should a data subject address a request to exercise one of their legal rights to the Controller, the Processor shall, if the Controller so requires, cooperate in the execution of this request. The Parties shall bear their own costs in this regard.

10 Secrecy and confidentiality

10.1 All personal data processed by the Processor on behalf of the Controller in the context of this DPA are subject to an obligation of confidentiality towards third parties. The Processor shall not use these personal data for any purpose other than that for which it has obtained them.

10.2 This secrecy obligation does not apply insofar as the Controller has given explicit permission to provide the personal data to third parties, provided that the disclosure of the personal data to third parties is logically necessary in view of the nature of the task assigned and the execution of this DPA, or if there is a legal obligation to provide the personal data to a third party.

11 Audit

11.1 The controller has the right to carry out audits by an independent third party bound by secrecy to verify compliance with the DPA.

11.2 This audit will only take place after the Controller has a concrete suspicion of misuse of Personal Data and has requested similar audit reports present at the Processor, assessed them and put forward reasonable arguments that justify an audit initiated by the Controller. Such an audit is justified if the similar audit reports present at the Processor do not provide any, or sufficient, evidence of the Processor's compliance with this DPA. The audit initiated by the Controller shall take place two weeks after it has been announced by the Controller, and no more than once a year.

11.3 Processor shall cooperate with the audit and share all information reasonably relevant to the audit as timely as possible. Processor shall ensure that the audit causes as little disruption as possible to the Processor's other activities.

11.4 The findings of the audit will be assessed by the Parties in mutual consultation and, as a result, may or may not be implemented by one or both Parties jointly. The costs of the audit will be borne by Controller.

12 Liability

12.1 The Parties respective liability for any breach of this DPA, including any damages resulting from a Personal Data Breach, shall be subject to the limitations and exclusions of liability set forth in the Contract.

12.2 Each Party is obliged to inform the other Party without undue delay of a (potential) liability claim or the (potential) imposition of a penalty by a Supervisory Authority, in connection with the DPA or otherwise. Parties are reasonably obliged to provide each other with information and/or support for the purpose of putting forward a defense against a (potential) liability claim or penalty, as referred to in the previous sentence. The Party that provides information and/or support shall be entitled to charge the other Party any potential reasonable costs in this respect; the Parties shall inform each other about these costs in advance as much as possible.

13 Duration, termination and deletion

13.1 This DPA shall enter into force upon signature by the Parties and on the date of the last signature.

13.2 This DPA has been entered into for the term specified in the Contract between the Parties and, in the absence thereof, for the duration of the processing of personal data of the Controller by the Data Processor.

13.3 Termination of this DPA will not exempt the Parties from their obligations arising from this DPA which by their nature are expected to continue after termination.

13.4 As soon as the DPA is terminated, for whatever reason and in whatever way, the Processor will, at the request of the Controller and within 60 business days, return all personal data in its possession in original or copy form to the Controller, and/or remove and/or destroy these original personal data and any copies thereof, if and to the extent still technically possible, unless applicable legislation requires storage of the Personal Data.

13.5 Processor shall on request give the Controller (written or electronic) confirmation that the deletion or return of the Personal Data has taken place.

13.6 Processor shall inform all Sub-processors involved in the Processing of Personal Data of a termination of this DPA and shall ensure that all Sub-processors will delete or return the Customer Personal Data.

14 Contradiction and amending the DPA

14.1 The order of precedence as described in the Contract is applicable in case of a contradiction between the articles of the DPA and the articles of other documents constituting the Contract.

14.2 Amendments to the articles of the DPA can be effected only by joint agreement between the Parties.

Appendix A: Specification of the processing of personal data

Description and applicability of the data processing activities

DataSnipper License	Features	Data processing activities
DataSnipper Start	Optical Character Recognition User Management System	Analytics & licensing Customer Relationship Management Cloud document analysis
DataSnipper Accelerate DataSnipper Elevate	Advanced Document Extraction DocuMine Optical Character Recognition UpLink AI User Management System	Analytics & licensing Customer Relationship Management Customer documents (AI) analysis Customer documents (AI) analysis
DataSnipper Add-ons	UpLink Document Portal Financial Statement Suite	Cloud storage Cloud document (AI) analysis

Overview of categories of personal data and data subjects:

Categories of personal data	Categories of data subjects
Full name E-mail address Job title IP-address Payment and billing information Customer Documents Customer Data User Data	Employees of customer's clients Freelancers of customer's client Customers of customer's clients Supplier of customer's clients Service providers of customer's clients

Overview of personal data categories processed per feature

Feature	Categories of personal data
Advanced Document Extraction	Customer Documents; Customer Data
Analytics & licensing	User Data
Customer Relationship Management	Full name; job title; e-mail address; payment and billing information
DocuMine	Customer Documents; Customer Data
Financial Statement Suite	Customer Documents; Customer Data
Optical Character Recognition	Customer Documents
UpLink AI	Customer Documents; Customer Data
UpLink PBC	Customer Documents; User Data
User Management System	Full name; e-mail address; IP-address

Appendix B: Procedure for the notification of a data breach

Contact details:

Contact details Controller	Contact details Processor
Primary Contact of Controller as indicated in Contract	legal@datasnipper.com

Should the Processor be unable to contact the aforementioned contact person for any reason, the Processor shall use the general e-mail address and telephone number. The Processor must provide Controller with the information below.

1. Discovery of the Data Breach by the Processor was discovered on [DATE] at [TIME].
2. The notification of the Data Breach to Controller took place on [DATE] at [TIME].
   [or]
   The notification of the Data Breach to Controller took place on [DATE] at [TIME], after the 72-hour period had elapsed after discovery, because [REASON OF LATE NOTIFICATION].
3. Measures taken by the Processor to mitigate the consequences of the Data Breach and prevent further/future Data Breaches:
   [LISTING OF MEASURES].
4. Other information relating to the Data Breach:
   - a description of the Data Breach;
   - the date on which the Data Breach occurred (if no exact date is known: the period during which the Data Breach occurred);
   - what the (alleged) cause of the Data Breach is;
   - what the (as yet known and/or expected) consequence is;
   - a description of the group of data subjects the Data Breach concerns;
   - the number of data subjects the Data Breach concerns (if no exact number is known: the minimum and maximum number of data subjects it concerns);
   - which categories of personal data have been affected by the Data Breach;
   - whether and how the personal data in question were secured (for example, by means of hashing or encryption) or made incomprehensible or inaccessible in any other way.

Appendix C: Technical and organizational measures

DataSnipper has implemented technical and organizational security measures in accordance with the controls described in its SOC 2 Type II report.

As part of the SOC 2 control framework, qualified and certified auditors have verified whether each control was suitably designed and operated effectively. The SOC 2 report contains the conclusions of the auditors.

As part of the controls that have been implemented, DataSnipper regularly reviews and updates the technical and organizational security measures protecting customer data, including personal data relating to persons authorized to use DataSnipper's solutions on behalf of the customer organization.

A subset of examples of technical and organizational security measures currently includes the following.

Data Protection and Encryption:

- All data in transit is encrypted using TLS 1.2+ protocols
- AES 256 encryption is used for data storage at rest
- User passwords are hashed and encrypted at rest

Access Control:

- Role-based access control (RBAC) is implemented
- Multi-factor authentication (MFA) is enforced

Infrastructure Security:

- Infrastructure is hosted in Microsoft Azure data centers, benefiting from Microsoft physical and logical security controls Continuous monitoring systems are in place for health, performance, and security
- Regular backups are performed with monitoring and alerts for failures

Compliance and Testing:

- Processor is SOC 2 compliant
- Annual penetration testing is conducted by external security professionals
- Regular vulnerability assessments and patch management

Employee Security:

- Mandatory security awareness training
- Regular phishing simulations and targeted follow-up training

Please note that these are not the only technical and organizational security measures taken, and e.g. encryption measures and algorithms will be updated when necessary to stay up-to-date with good information security and privacy practices.