DATA PROCESSING AGREEMENT

Standard form · Version 1.2 · September 2026

This Data Processing Agreement (the "**DPA**") forms part of and is subject to the agreement governing the Customer's use of the Services (the "**Principal Agreement**") between:

(1) [Customer legal name], a company registered in [jurisdiction] under number [registration number], with its registered office at [address] (the "**Controller**" or "**Customer**"); and

(2) FLUIDLABS OÜ, a company registered in Estonia under registry code 16534086, with its registered office at Vesivärava tn 50-201, 10152 Tallinn, Estonia (the "**Processor**" or "**Fluidlabs**").

each a "**Party**" and together the "**Parties**".

---

1. Definitions

1.1 Terms used but not defined in this DPA have the meaning given to them in the Principal Agreement or, where relevant, in Data Protection Law.

1.2 In this DPA:

- "**Data Protection Law**" means all laws applicable to the processing of Personal Data under this DPA, including Regulation (EU) 2016/679 (the "**GDPR**"), the GDPR as incorporated into the law of the United Kingdom (the "**UK GDPR**") together with the Data Protection Act 2018, and the Swiss Federal Act on Data Protection, in each case as amended or replaced.
- "**Customer Personal Data**" means Personal Data that Fluidlabs processes on behalf of the Customer in the course of providing the Services.
- "**EU SCCs**" means the standard contractual clauses annexed to European Commission Implementing Decision (EU) 2021/914.
- "**Personal Data**", "**processing**", "**controller**", "**processor**", "**data subject**", "**personal data breach**" and "**supervisory authority**" have the meanings given in the GDPR.
- "**Restricted Transfer**" means a transfer of Customer Personal Data to a country that is not the subject of an adequacy decision under the applicable Data Protection Law.
- "**Services**" means the services described in the Principal Agreement, including the Docusign extension applications developed, hosted or supported by Fluidlabs for the Customer.
- "**Subprocessor**" means any third party engaged by Fluidlabs to process Customer Personal Data.
- "**UK Addendum**" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018.

---

2. Roles of the Parties and scope

2.1 The Parties acknowledge that, for the purposes of this DPA, the Customer is the controller and Fluidlabs is the processor in respect of Customer Personal Data. Where the Customer is itself a processor acting for a third-party controller, Fluidlabs acts as a subprocessor and this DPA applies as if references to the Customer's obligations as controller were references to the obligations it owes to that third-party controller.

2.2 Fluidlabs processes Personal Data relating to the Customer's own account contacts for its own account and administrative purposes, such as contract management and billing. Fluidlabs is an independent controller for that limited processing, and it is not Customer Personal Data under this DPA.

2.3 The subject matter, duration, nature and purpose of the processing, the types of Personal Data and the categories of data subject are set out in **Annex I**.

2.4 This DPA applies from the date of the Principal Agreement and continues for as long as Fluidlabs processes Customer Personal Data.

---

3. Processing on documented instructions

3.1 Fluidlabs shall process Customer Personal Data only on the Customer's documented instructions, including with regard to transfers to a third country, unless required to do otherwise by Union or Member State law to which Fluidlabs is subject. Where such a legal requirement applies, Fluidlabs shall inform the Customer of that requirement before processing, unless the law prohibits it on important grounds of public interest.

3.2 The Principal Agreement, this DPA and the Customer's use and configuration of the Services constitute the Customer's complete documented instructions. Any additional or different instruction must be agreed in writing and may be subject to reasonable charges where it requires work outside the scope of the Services.

3.3 Fluidlabs shall promptly inform the Customer if, in its opinion, an instruction infringes Data Protection Law. Fluidlabs may suspend the affected processing until the instruction is confirmed, amended or withdrawn.

3.4 The Customer warrants that it has a lawful basis for the processing it instructs, that it has provided all required information to data subjects, and that its instructions comply with Data Protection Law. The Customer is responsible for the accuracy, quality and legality of the Customer Personal Data it makes available to Fluidlabs.

3.5 The Customer shall not make special categories of Personal Data within the meaning of Article 9 GDPR, or Personal Data relating to criminal convictions and offences, available to Fluidlabs unless the Parties have agreed this in writing in advance and recorded it in Annex I.

---

4. Confidentiality

4.1 Fluidlabs shall treat Customer Personal Data as confidential and shall not disclose it except as permitted by this DPA or required by law.

4.2 Fluidlabs shall ensure that every person authorised to process Customer Personal Data is bound by an enforceable contractual obligation of confidentiality that survives the end of their engagement, and has received appropriate training on their obligations.

4.3 Fluidlabs shall limit access to Customer Personal Data to those personnel who need it in order to perform the Services.

---

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk to the rights and freedoms of natural persons, Fluidlabs shall implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, as required by Article 32 GDPR.

5.2 The measures in force at the date of this DPA are described in **Annex II**. Fluidlabs may update those measures from time to time provided that the overall level of security is not reduced.

5.3 Fluidlabs maintains certification to ISO/IEC 27001:2022 and shall use reasonable efforts to maintain equivalent certification for the term of this DPA.

---

6. Subprocessors

6.1 The Customer grants Fluidlabs general written authorisation to engage Subprocessors, subject to this clause 6.

6.2 The Subprocessors authorised at the date of this DPA are listed in **Annex III**.

6.3 Fluidlabs shall give the Customer at least **thirty (30) days'** notice before adding or replacing a Subprocessor. Notice will be given to the Customer's notification contact recorded in Annex I.

6.4 The Customer may object to a proposed Subprocessor on reasonable data protection grounds by giving written notice within the notice period. The Parties shall discuss the objection in good faith. If Fluidlabs cannot make available a commercially reasonable alternative within a reasonable period, either Party may terminate the affected part of the Services on written notice, without liability, and the Customer shall be refunded any prepaid fees for the terminated portion covering the period after termination.

6.5 Fluidlabs shall impose on each Subprocessor, by written contract, data protection obligations that are no less protective than those set out in this DPA, and shall remain fully liable to the Customer for the performance of each Subprocessor's obligations.

6.6 On request, Fluidlabs shall provide the Customer with a copy of the data protection terms of its agreement with any Subprocessor, which may be redacted to remove commercial terms.

---

7. Data subject rights

7.1 Taking into account the nature of the processing, Fluidlabs shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, to fulfil the Customer's obligation to respond to requests from data subjects exercising their rights under Chapter III GDPR.

7.2 If Fluidlabs receives a request directly from a data subject relating to Customer Personal Data, it shall not respond to the substance of the request. Fluidlabs shall forward the request to the Customer without undue delay and, where reasonably possible, within **five (5) business days**, and shall follow the Customer's instructions in dealing with it.

---

8. Assistance with the Customer's obligations

8.1 Fluidlabs shall assist the Customer, taking into account the nature of the processing and the information available to Fluidlabs, in ensuring compliance with the Customer's obligations under Articles 32 to 36 GDPR, covering security of processing, personal data breach notification, data protection impact assessments and prior consultation with a supervisory authority.

8.2 Fluidlabs shall make available to the Customer all information reasonably necessary to demonstrate compliance with Article 28 GDPR.

8.3 Assistance under clauses 7 and 8 is provided at no additional charge where the request is proportionate and relates to the Services. Where assistance requires substantial effort beyond that, Fluidlabs may charge on a time and materials basis at its then-current rates, notified in advance.

---

9. Personal data breach

9.1 Fluidlabs shall notify the Customer without undue delay, and in any event **within forty-eight (48) hours**, after becoming aware of a personal data breach affecting Customer Personal Data.

9.2 The notification shall describe, to the extent known at the time and supplemented as further information becomes available:

- (a) the nature of the breach, including where possible the categories and approximate number of data subjects and records concerned;
- (b) the contact point for further information;
- (c) the likely consequences of the breach; and
- (d) the measures taken or proposed to address the breach and mitigate its effects.

9.3 Fluidlabs shall take reasonable steps to contain and investigate the breach, shall document all breaches affecting Customer Personal Data, and shall cooperate with the Customer in its handling of the breach.

9.4 Fluidlabs shall not notify a supervisory authority or any data subject of a breach affecting Customer Personal Data on the Customer's behalf unless the Customer instructs it to do so, or unless Fluidlabs is required to do so by law.

9.5 Notification of a breach under this clause is not an acknowledgement by Fluidlabs of fault or liability.

---

10. Deletion and return

10.1 On termination or expiry of the Principal Agreement, or earlier at the Customer's written request, Fluidlabs shall at the Customer's choice delete or return all Customer Personal Data and delete existing copies, unless Union or Member State law requires it to be retained.

10.2 The Customer shall make its election within **thirty (30) days** of termination or expiry. If the Customer makes no election within that period, Fluidlabs shall delete the Customer Personal Data.

10.3 Customer Personal Data held in encrypted backups shall be deleted on the expiry of the applicable backup retention cycle, and shall remain subject to this DPA until it is deleted.

10.4 On request, Fluidlabs shall provide written confirmation that it has complied with this clause.

---

11. Audit

11.1 Fluidlabs shall make available to the Customer, on reasonable written request and no more than once in any twelve (12) month period, the information necessary to demonstrate compliance with this DPA.

11.2 The Customer accepts that Fluidlabs may discharge its obligation under clause 11.1 by providing its current ISO/IEC 27001:2022 certificate and responses to a reasonable written security questionnaire.

11.3 Where the information provided under clause 11.2 is not sufficient to demonstrate compliance, or following a personal data breach affecting Customer Personal Data, or where a supervisory authority requires it, the Customer may carry out an audit or mandate an independent auditor to do so. Any such audit shall:

- (a) be preceded by at least thirty (30) days' written notice, except where a supervisory authority requires otherwise;
- (b) take place during normal business hours and be conducted so as to cause minimum disruption;

- (c) not extend to any data, systems or premises relating to other customers of Fluidlabs;
- (d) be subject to the auditor signing a confidentiality undertaking reasonably acceptable to Fluidlabs, and the auditor not being a competitor of Fluidlabs; and
- (e) be at the Customer's cost, unless the audit reveals a material breach of this DPA by Fluidlabs, in which case Fluidlabs shall bear its own costs and reimburse the Customer's reasonable costs.

11.4 The audit rights in this clause do not extend to the premises or systems of Fluidlabs' Subprocessors. In respect of those, Fluidlabs shall provide the relevant third-party audit reports and certifications available to it.

---

12. International transfers

12.1 Fluidlabs shall not transfer Customer Personal Data to a country outside the European Economic Area, or grant access to it from such a country, except in accordance with this clause.

12.2 Where a Restricted Transfer takes place, the Parties agree that the **EU SCCs** apply and are incorporated into this DPA by reference, on the following basis:

- **Module Two (controller to processor)** applies, or **Module Three (processor to processor)** where the Customer acts as a processor for a third-party controller;
- Clause 7 (docking clause) applies;
- in Clause 9, **Option 2 (general written authorisation)** applies, with the notice period specified in clause 6.3 of this DPA;
- in Clause 11, the optional independent dispute resolution paragraph does not apply;
- in Clause 17, the governing law is the law of **Estonia**;
- in Clause 18(b), the forum is the courts of **Estonia**;
- Annex I, Annex II and Annex III of the EU SCCs are populated by Annex I, Annex II and Annex III of this DPA respectively.

12.3 For transfers subject to the UK GDPR, the **UK Addendum** applies to the EU SCCs. Table 1 is populated by Annex I of this DPA, Tables 2 and 3 by clause 12.2 and the Annexes of this DPA, and in Table 4 neither Party may end the Addendum as set out in Section 19.

12.4 For transfers subject to Swiss law, references in the EU SCCs to the GDPR are to be understood as references to the Swiss Federal Act on Data Protection, the competent authority is the Swiss Federal Data Protection and Information Commissioner, and the term "Member State" shall not be interpreted so as to exclude data subjects in Switzerland from enforcing their rights in their place of habitual residence.

12.5 The Parties acknowledge that Customer Personal Data is hosted with the Subprocessors identified in Annex III, including hosting infrastructure located in the United States. Each such Restricted Transfer is subject to the EU SCCs as incorporated by clause 12.2, together with the supplementary measures described in Annex II.

12.6 If the transfer mechanism relied on under this clause is invalidated, or ceases to provide an adequate level of protection, the Parties shall work together in good faith to put in place an alternative lawful transfer mechanism without undue delay.

---

13. Liability

13.1 The liability of each Party under or in connection with this DPA is subject to the limitations and exclusions of liability set out in the Principal Agreement.

13.2 Nothing in this DPA limits or excludes either Party's liability to a data subject or a supervisory authority under Data Protection Law.

---

14. General

14.1 **Order of precedence.** In the event of a conflict between this DPA and the Principal Agreement, this DPA prevails in respect of the processing of Customer Personal Data. In the event of a conflict between this DPA and the EU SCCs, the EU SCCs prevail.

14.2 **Term.** This DPA takes effect on the effective date of the Principal Agreement and terminates automatically when Fluidlabs ceases to process Customer Personal Data and has complied with clause 10.

14.3 **Variation.** Any variation to this DPA must be in writing and signed by both Parties, except that Fluidlabs may update Annex II and Annex III in accordance with clauses 5.2 and 6.3.

14.4 **Severability.** If any provision of this DPA is held to be invalid or unenforceable, the remainder continues in full force.

14.5 **Governing law.** This DPA is governed by the laws of **Estonia**, and the courts of **Tallinn, Estonia** have exclusive jurisdiction, without prejudice to clauses 12.2 and 12.3.

ANNEX I

Description of the processing

A. List of Parties

Data exporter (Controller)

Field	Detail
Name	[Customer legal name]
Address	[address]
Contact person	[name, role, email]
Data protection contact / DPO	[name and email, or "not appointed"]
Notification contact for clause 6.3	[email]
Activities relevant to the transfer	Use of the Docusign extension applications provided by Fluidlabs
Role	Controller (or processor, where acting for a third-party controller)

Data importer (Processor)

Field	Detail
Name	FLUIDLABS OÜ (registry code 16534086)
Address	Vesivärava tn 50-201, 10152 Tallinn, Estonia
Contact	Security & Compliance, secops@fluidlabs.com
Data protection contact	secops@fluidlabs.com
Activities relevant to the transfer	Development, hosting, operation and support of Docusign extension applications
Role	Processor

B. Description of the processing

Item	Detail
Subject matter	Provision of the Docusign extension applications and related support services described in the Principal Agreement.
Duration	The term of the Principal Agreement, plus the retention and deletion period set out in clause 10.
Nature and purpose	Receiving, storing, transforming and transmitting data between the Customer's Docusign environment and the systems the extension application connects to, so that the Customer's document and agreement workflows operate as configured; together with support, error investigation and maintenance of the application.

Categories of data subject	To be completed per engagement. Typically: the Customer's employees and other personnel whose records are processed through the connected systems; signers, recipients and other parties named in the Customer's Docusign envelopes; users of the application.
Categories of Personal Data	To be completed per engagement. Typically: identification and business contact data (name, work email address, job title, organisation); employment record fields made available by the Customer's connected system to the extent required by the configured workflow; envelope and agreement metadata including document titles, status, timestamps and audit-trail entries; any Personal Data contained in documents processed through the application; application and access logs.
Special category data	None. The Customer shall not make special category data available to Fluidlabs unless the Parties agree it in writing and record it here.
Frequency of transfer	Continuous, for the duration of the Principal Agreement.
Retention	Customer Personal Data is retained for the term of the Principal Agreement and deleted in accordance with clause 10. Log and backup retention periods are stated at signature.
Subprocessor processing	As set out in Annex III, for the purpose and duration stated there.

C. Competent supervisory authority

The supervisory authority of the Member State in which the Customer is established. Where the Customer is not established in the EEA but has appointed a representative under Article 27 GDPR, the supervisory authority of the Member State in which that representative is established. Where neither applies, the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon).

ANNEX II

Technical and organisational measures

The following measures are in force at the date of this DPA. They are maintained within an information security management system certified to ISO/IEC 27001:2022, which also governs Fluidlabs' handling of personal data in accordance with the GDPR.

1. Pseudonymisation and encryption

- All Customer Personal Data in transit over public networks is protected with TLS 1.2 or higher.
- All Customer Personal Data at rest, including backups, is encrypted using AES-256.
- Encryption keys are managed through the cloud provider's key management service, with access restricted to authorised administrators.
- Credentials, API keys and tokens are held in a dedicated secrets manager and are never committed to source control.

2. Confidentiality and access control

- Identity is centralised in a single directory. Multi-factor authentication is enforced for all personnel accounts.
- Access to production systems and Customer Personal Data is granted by role, on a least-privilege and need-to-know basis, and requires documented approval.
- Administrative access to production infrastructure is limited to named individuals.
- Access rights are reviewed and signed off at least quarterly, with discrepancies logged and remediated.
- Access is revoked within 24 hours of a person leaving or changing role. Shared or non-MFA credentials are rotated as part of the same procedure.
- Remote access to infrastructure is through an authenticated private network.

3. Integrity

- All code changes are made through pull requests in a version-controlled repository, require review by a second person, and are blocked from being pushed directly to protected branches.
- Automated checks run on every change before it can be merged.
- File integrity monitoring is deployed on the hosting infrastructure.
- Production is logically separated from development environment, and production data is not copied into non-production environment.

4. Availability and resilience

- Customer Personal Data is hosted on Amazon Web Services, which provides redundant infrastructure and physical and environmental controls.
- Backups are taken on a scheduled cycle, encrypted, and restoration is tested as part of the disaster recovery exercise.
- A business continuity plan and disaster recovery plan are maintained, with documented test reports.

5. Testing and evaluation of effectiveness

- Cloud configuration is assessed weekly against industry benchmarks (CIS) using automated tooling, with results retained.
- Vulnerability detection and security configuration assessment run continuously on the hosting infrastructure.

- Penetration testing is performed by an independent third party, with findings tracked to remediation.
- Internal audits and a management review of the information security management system are performed on a documented annual cycle.

6. Logging and monitoring

- Security-relevant events across infrastructure and applications are collected into a centralised monitoring platform.
- Logs are protected against unauthorised modification and retained for a defined period stated at signature.
- Alerts are reviewed on a documented cycle and escalated through the incident response procedure.

7. Incident management

- A documented incident response policy defines roles, severity classification, escalation and communication.
- All incidents are recorded in an incident log with their classification, handling and resolution.
- Personal data breaches affecting Customer Personal Data are notified to the Customer within 48 hours of Fluidlabs becoming aware of them.

8. Personnel

- All personnel are bound by written confidentiality obligations that survive the end of their engagement.
- Identity and reference verification is performed at onboarding. Additional screening is performed where required by a client contract.
- Security awareness training is delivered at onboarding and refreshed annually, with records retained.
- All personnel formally acknowledge the acceptable use, access control and data protection policies.
- Onboarding and offboarding follow a documented procedure with recorded, per-system access changes.

9. Endpoint and physical security

- Personnel devices are company-controlled, encrypted at rest, and protected by screen lock and endpoint protection software.
- Fluidlabs operates a remote-first model. Physical and environmental controls for the systems holding Customer Personal Data are provided by the cloud subservice organisations, whose certifications are reviewed annually.

10. Supplier and subprocessor management

- All suppliers with access to Customer Personal Data are recorded in a supplier register with a documented security assessment and an annual review date.
- Suppliers are assessed against criteria including certification, encryption at rest and in transit, multi-factor authentication, logging and monitoring, and availability commitments.
- Data processing terms are in place with each Subprocessor that are no less protective than this DPA.

11. Data minimisation, retention and deletion

- The application processes only the data required for the configured workflow.
- Retention periods are defined per data category and applied on expiry.
- Deletion on termination follows clause 10, with backup copies removed on the expiry of the backup retention cycle.

12. Supplementary measures for transfers

- Access to Customer Personal Data from outside the EEA is limited to named personnel, requires multi-factor authentication and passes through an authenticated private network.
- Such access is logged and included in the quarterly access review.
- Fluidlabs maintains a policy of challenging any government or law enforcement request for Customer Personal Data where there is a lawful basis to do so, and of notifying the Customer of any such request unless legally prohibited.
- Fluidlabs has received no government request for access to Customer Personal Data as at the date of this DPA.

ANNEX III

Authorised Subprocessors

#	Subprocessor	Registered location	Purpose	Location of processing	Safeguard
1	Amazon Web Services, Inc.	United States	Cloud hosting of the application, database and backups	United States, US East (N. Virginia) region	AWS DPA incorporating the EU SCCs; ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2
2	Cloudflare, Inc.	United States	DNS, TLS termination, web application firewall, DDoS protection	Global edge network	Cloudflare DPA incorporating the EU SCCs; ISO 27001, ISO 27018, ISO 27701
3	Google LLC (Google Workspace)	United States	Business communication and file storage used in support activities	EU and United States	Google DPA incorporating the EU SCCs; ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2
4	Datadog, Inc.	United States	Infrastructure monitoring and application log management	United States	Datadog DPA incorporating the EU SCCs; ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC 2

Fluidlabs personnel access Customer Personal Data in the course of providing the Services. This is not subprocessing, and is addressed in clause 12.5 and section 12 of Annex II.

An up-to-date list of Subprocessors is available on request from secops@fluidlabs.com.

Signatures

For and on behalf of [Customer legal name]

Name: .....

Title: .....

Signature: .....

Date: .....

For and on behalf of FLUIDLABS OÜ

Name: Shamil Malachiyev

Title: Chief Executive Officer

Signature: .....

Date: .....