Data Processing Agreement

Last updated: January 2025

This Data Processing Agreement, including all appendices (hereinafter: "Data Processing Agreement"), is entered into between Setflow B.V. and Client. The Setso Terms of Use form an integral part of this Data Processing Agreement.

Article 1. Definitions

- **1.1 "GDPR"**: the General Data Protection Regulation (Regulation 2016/679/EU).
- **1.2 "Data Subject"**: the natural person to whom a Personal Data relates.
- **1.3 "Data Breach"**: a breach of security which, accidentally or unlawfully, results in the destruction, loss, alteration or unauthorized disclosure of, or unauthorized access to, transmitted, stored or otherwise processed Personal Data.
- **1.4 "Main Agreement"**: the agreement entered into by the Controller and the Processor for the provision of services by the Processor, of which the Data Processing Agreement forms a part.
- **1.5 "Client"**: the natural person or legal entity that is designated as such in the Main Agreement.
- **1.6 "Personal Data"**: all information relating to an identified or identifiable natural person, as described in Article 4(1) of the GDPR.
- **1.7 "Sub-Processor"**: the natural person or legal entity that assists a Processor in processing Personal Data on behalf of the Controller.
- **1.8 "Controller"**: the natural person, legal entity, or any other body that determines the purpose and means for the Processing of Personal Data.
- **1.9 "Processing"**: any operation or set of operations performed on Personal Data.
- **1.10 "Processor"**: a natural person or legal entity which processes Personal Data on behalf of a Controller.

Article 2. Roles of the Parties

2.1 The Parties agree that with respect to the Processing of Personal Data pursuant to the Main Agreement, Setflow B.V. is designated as the Processor within the meaning of the GDPR.

2.2 The Parties agree that the Client is designated as the Controller within the meaning of the GDPR.

Article 3. General

3.1 This Data Processing Agreement applies exclusively to the Processing of Personal Data by the Processor on behalf of the Controller in the context of the Main Agreement.

3.2 This Data Processing Agreement forms an integral part of the Main Agreement. All rights and obligations arising from the Main Agreement, including limitations of liability, shall therefore also apply.

3.3 Annex I includes: the Personal Data that may be processed; the retention period; the categories of Data Subjects; the Sub-Processors; and the nature and purpose of the Processing.

Article 4. Processing of Personal Data

4.1 The Processor processes Personal Data solely for the execution of the Main Agreement and other instructions agreed in writing with the Controller.

4.2 The Processor shall process only the Personal Data specified in Annex I, within the scope of the nature and purposes described in that Annex.

4.3 The Processor shall follow all reasonable instructions from the Controller and immediately inform the Controller if any instruction is in conflict with applicable legislation.

4.4 The Processor shall provide assistance to the Controller in complying with the obligations pursuant to Articles 32 to 36 of the GDPR.

4.5 The Controller guarantees that the Processing of Personal Data by the Processor under this Agreement is not in conflict with data protection legislation. The Controller indemnifies the Processor for all related claims, damages, and fines.

Article 5. Technical and Organizational Security Measures

5.1 The Processor shall take appropriate technical and organizational security measures as described in Annex II, to secure the Personal Data against a Data Breach.

5.2 The Processor grants its personnel access to the Personal Data only to the extent strictly necessary. All individuals participating in the Processing are bound by a confidentiality obligation.

Article 6. Data Breach

6.1 The Processor shall inform the Controller as soon as possible after detecting a Data Breach and take measures to remedy it and minimize its consequences.

6.2 The Processor shall provide the Controller with all information necessary to comply with Article 33 of the GDPR.

6.3 It is solely for the Controller to determine whether a Data Breach is to be reported to the Data Protection Authority and/or Data Subjects.

Article 7. Sub-Processors

7.1 The Processor has general permission to engage Sub-Processors as listed in Annex I. The Processor shall notify the Controller in writing at least 14 days in advance of any changes to the Sub-Processor list.

7.2 The Processor shall ensure that its Sub-Processors are contractually bound to equivalent obligations.

7.3 The Processor remains fully responsible for the actions of the Sub-Processor.

Article 8. Retention Periods

8.1 The Controller is responsible for determining the retention periods as set out in Annex I.

8.2 The Processor shall delete the Personal Data within 60 days after the termination of the Agreement or, at the Controller's option, transfer it to the Controller.

Article 9. International Transfer of Personal Data

9.1 The Processor may not transfer any Personal Data to countries outside the EEA unless:

- the Controller has given prior written consent; or
- there is an adequacy decision by the European Commission; or
- the transfer is made on the basis of EU Standard Contractual Clauses; or
- the transfer is made on the basis of binding corporate rules as referred to in Article 47 of the GDPR.

Article 10. Rights of Data Subjects

10.1 If the Controller has direct access to the Personal Data, it shall respond to all Data Subject requests without support from the Processor.

10.2 The Processor shall cooperate with reasonable requests relating to Data Subject rights under the GDPR.

10.3 The Processor shall cooperate with DPIA assessments as referred to in Articles 35 and 36 of the GDPR.

10.4 The Processor shall cooperate with requests for deletion or correction of Personal Data.

Article 11. Audit

11.1 Upon request, the Processor shall enable the Controller to verify compliance with this Agreement.

11.2 The Processor shall make available all information necessary to demonstrate compliance with Article 28 of the GDPR.

11.3 The Controller shall treat all information found during the audit confidentially.

Article 12. Other Provisions

12.1 Amendments to this Data Processing Agreement shall only be valid if agreed in writing.

12.2 The Parties shall adjust this Agreement to changes in legislation, additional instructions from relevant authorities, and developments in the application of the GDPR.

Annex I — Processing of Personal Data

I. Categories of Personal Data

- First Name, Last Name, Middle Name/Prefix
- Date of Birth
- Email Address, Telephone Number, Address
- Dietary Preferences
- Clothing Sizes
- Gender (optional) and/or Gender identity
- Position/Role
- In Case of Emergency number
- Agent/Company connected to this person
- Kilometers driven (possibly with which car)
- Hours worked, Overtime worked
- Impression of how the day was for this person (emoticon)

II. Categories of Data Subjects

- Employees of the Controller
- Self-employed persons and (small) companies providing services to the Controller
- Participants (natural persons) in production/project who are not directly employees

III. Nature and Purpose of the Processing

The Processor processes the Personal Data solely for the purpose of being able to offer its services pursuant to the Main Agreement and to develop and improve its services.

IV. Retention Periods

All Personal Data, with the exception of first name, last name, and position/role, shall be retained only for the duration of the Main Agreement. First name, last name, and position/role shall be retained as long as necessary to generally develop, improve, and deliver services.

V. Sub-Processors

Sub-Processor	Country	Service	Purpose	Data	Storage
Microsoft Ireland Operations Limited	Ireland	Azure	Cloud and VPN provider	All	EU
MongoDB, Inc.	United States	MongoDB	Database for the Setso platform, hosted by Azure	All	EU
PostHog, Inc.	United States	PostHog	Product analytics platform	User data	EU
Clerk, Inc.	United States	Clerk	User management and authentication	User data	EU
Attio, Ltd.	United Kingdom	Attio	Customer Relationship Management (CRM)	Customer data	EU
Sequence Financial Technology Ltd.	United Kingdom	Sequence	Billing and subscription management	Customer & payment data	EU
Stripe, Inc.	United States	Stripe	Payment processing services	Payment data	EU

Annex II — Technical and Organizational Measures

- Security software, such as antivirus and firewall.
- TLS (formerly SSL): Personal Data is transmitted via a secure internet connection.
- DKIM, SPF, and DMARC: Three internet standards used to prevent phishing and spoofed emails.
- Encryption on local drives of the Processor.
- Accounts available via the Website are secured with passwords and MFA; accounts available via the App are secured with PIN code and/or biometric security.
- The IT environment is regularly monitored for unusual activities.
- The Processor conducts penetration/hack tests at regular intervals.