Data Processing Agreement

Version 2.2 · October 2026

BETWEEN

FlatTurtle BV, a private limited company under Belgian law, with registered office at Ikaroslaan 1, 1930 Zaventem, Belgium, registered with the Crossroads Bank for Enterprises under number VAT BE 0843.961.762 (the **Processor**);

acting in the capacity of Processor;

AND

The Customer as defined in the General Terms and Conditions of Processor (the **Controller**);

acting in the capacity of Controller;

each a **Party** and collectively the **Parties**.

Background

(A) The Controller and the Processor entered into an agreement regarding products and services delivered/ rendered by the Controller (the **Master Agreement**) that may require the Processor to process Personal Data on behalf of the Controller.

(B) This Data Processing Agreement (the **DPA**) sets out the additional terms, requirements and conditions on which the Processor will process Personal Data when providing services under the Master Agreement. This DPA contains the mandatory clauses required by Article 28(3) of the GDPR for contracts between controllers and processors.

(C) This DPA is validly concluded at the moment both the Controller and the Processor accept the quotation of the Controller.

Agreed terms

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this DPA.

1.1 Definitions:

Business Purposes means the services described in the Master Agreement and/or any other purpose specifically identified in Annex A.

Data Protection Legislation means the GDPR and the applicable implementation legislation under Belgian law.

GDPR means Regulation (EU) 2016/679 of the European Parliament and of Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Controller, **Data Protection Impact Assessment**, **Data Subject**, **Personal Data**, **Personal Data Breach**, **process(ing)** and **Processor** shall have the same meaning as in the GDPR.

1.2 This DPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement.

1.3 In the case of conflict or ambiguity between:

1.3.1 any provision contained in the body of this DPA and any provision contained in the Annexes, the provision in the body of this DPA will prevail; and

1.3.2 any of the provisions of this DPA and the provisions of the Master Agreement, the provisions of this DPA will prevail.

2. Personal Data types and processing purposes

2.1 The Controller retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to the Processor. The Controller shall inform the Processor of any additional national and/or sector-specific mandatory legislation that applies to the processing by the Processor as a result of the processing by the Controller.

2.2 Annex A describes the nature and purpose of processing, the retention term(s) and the Personal Data categories and Data Subject types in respect of which the Processor may process to fulfil the Business Purposes.

3. Processor's obligations

3.1 The Processor will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Controller's written instructions. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this DPA or the Data Protection Legislation. The Processor must promptly notify the Controller if, in its opinion, the Controller's instruction would not comply with the Data Protection Legislation.

3.2 The Processor will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Controller or this DPA specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires the Processor to process or disclose Personal Data, the Processor must first inform the Controller of the legal or regulatory requirement and give the Controller an opportunity to object or challenge the requirement, unless the law prohibits such notice.

3.3 The Processor will reasonably assist the Controller with meeting the Controller's compliance obligations under the Data Protection Legislation, taking into account the nature of the Processor's processing and the information available to the Processor, including in relation to Data Subject rights, Data Protection Impact Assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

3.4 The Processor shall be entitled to full compensation for the assistance mentioned in Article 3.3, unless this assistance is the result of a proven non-compliance by the Processor with this DPA or the Data Protection Legislation.

4. Processor's employees

4.1 The Processor will ensure that all employees:

4.1.1 are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data; and

4.1.2 are aware of the Processor's duties and their personal duties and obligations under the Data Protection Legislation and this DPA.

5. Security

5.1 The Processor must implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data, as further described in Annex B.

5.2 The Processor must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

5.2.1 the pseudonymisation and encryption of personal data;

5.2.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.2.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

5.2.4 a process for regularly testing, assessing and evaluating the effectiveness of security measures.

6. Personal Data Breach

6.1 The Processor will without undue delay notify the Controller if it becomes aware of a Personal Data Breach.

6.2 Where the Processor becomes aware of a Personal Data Breach, it shall, without undue delay, also provide the Controller with the following information:

6.2.1 description of the nature thereof, including the categories and approximate number of both Data Subjects and Personal Data records concerned;

6.2.2 the likely consequences; and

6.2.3 description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

6.3 Immediately following a Personal Data Breach, the Parties will co-ordinate with each other to investigate the matter. The Processor will reasonably co-operate with the Controller in the Controller's handling of the matter, including:

6.3.1 assisting with any investigation;

6.3.2 taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach.

6.4 The Processor will not inform any third party of any Personal Data Breach without first obtaining the Controller's prior written consent, except when required to do so by law.

6.5 The Controller shall cover all reasonable expenses associated with the Processor's performance under this Clause 6 unless the matter arose from the Processor's negligence, wilful misconduct or breach of this DPA.

7. Cross-border transfers of Personal Data

7.1 The Processor (or any Sub-Processor) shall only transfer or otherwise process Personal Data outside the European Economic Area (EEA) if the Processor (or the Sub-Processor) has provided appropriate safeguards in accordance with Article 46 GDPR, or if such transfer is mandatory under EU or EU member state provisions.

7.2 Where appropriate, the Processor (or the Sub-Processor) shall conclude EU Standard Contractual Clauses adopted by the European Commission with the data importer outside the EEA.

8. Subcontractors

8.1 The Processor may only authorise a third party (the **Sub-Processor**) to process the Personal Data if:

8.1.1 the Sub-Processor has a profile similar to the Sub-Processor(s) approved at the commencement of this DPA; and

8.1.2 the Processor enters into a written contract with the Sub-Processor that contains terms substantially the same as those set out in this DPA, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Controller's written request, provides the Controller with copies of such contracts.

8.2 Those Sub-Processors approved at the commencement of this DPA are as set out in Annex A. The Processor must list all approved subcontractors in Annex A and include any Sub-Processor's name, location and contact information for the person responsible for data protection compliance.

8.3 Without prejudice to Clause 13.1, the Processor shall remain fully liable to the Controller for any failure by a Sub-Processor to fulfil its obligations in relation to the processing of the Personal Data.

9. Complaints, Data Subject requests and third-party rights

9.1 The Processor must take such technical and organisational measures as agreed in writing between the Parties, and promptly provide such information to the Controller as the Controller may reasonably require, to enable the Controller to comply with:

9.1.1 the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

9.1.2 information or assessment notices served on the Controller by any supervisory authority under the Data Protection Legislation.

9.2 The Processor must notify the Controller immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either Party's compliance with the Data Protection Legislation.

9.3 The Processor must notify the Controller within 5 working days if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

9.4 The Processor will reasonably cooperate with, and assist, the Controller in responding to any complaint, notice, communication or Data Subject request.

9.5 The Processor shall be entitled to full compensation for the assistance mentioned in Article 9.4, unless this assistance is the result of a proven non-compliance by the Processor with this DPA or the Data Protection Legislation.

9.6 The Processor must not disclose the Personal Data to any Data Subject or to a third party other than at the Controller's request or instruction, as provided for in this DPA or as required by law.

10. Term and termination

10.1 This DPA will remain in full force and effect so long as:

10.1.1 the Master Agreement remains in effect; or

10.1.2 the Processor retains any Personal Data related to the Master Agreement in its possession or control (the **Term**).

10.2 Any provision of this DPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement (including, but not limited to, Clause 13.1) will remain in full force and effect.

11. Data return and destruction

11.1 On termination of the Master Agreement for any reason or expiry of its term, the Processor will securely delete or destroy or, if directed in writing by the Controller, return and not retain, all or any Personal Data related to this DPA in its possession or control.

11.2 If any law, regulation, or government or regulatory body requires the Processor to retain any documents or materials that the Processor would otherwise be required to return or destroy, it will notify the Controller in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends.

11.3 The Processor will, at the Controller's first request, certify in writing that it has destroyed the Personal Data within 14 days after it completes the destruction.

12. Audit

12.1 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations under this DPA and the Data Protection Legislation and allow the Controller and its authorized auditors to perform audits regarding the compliance by the Processor with its obligations under this DPA and the Data Protection Legislation.

12.2 Any such audit may not take place more than once every contract year, shall be at the sole expense of the Controller and shall be subject to the Controller providing the Processor with at least thirty (30) days prior written notice of its intention to perform an audit. The audit shall take place during the normal business hours and shall not unreasonably interfere with the Processor's business activities. The Processor shall have the right to require Controller and any third-party auditor to enter into a non-disclosure agreement prior to performing the audit.

13. Miscellaneous

13.1 To the extent permitted under applicable law, any limitations and/or exclusions of liability in the Master Agreement are applicable to this DPA.

13.2 If at any time during the Term, one of the provisions of this DPA, is determined to be or to have become invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions of the DPA shall not in any way be affected or impaired. The Parties shall negotiate in good faith to replace such invalid, illegal or unenforceable provision with a valid, legal and enforceable provision the effect of which comes as close as possible to that of the invalid, illegal or unenforceable provision.

13.3 This DPA will be governed by, and construed in accordance with, the laws applicable to the Master Agreement. The same court as stated in the Master Agreement shall have exclusive jurisdiction for any disputes arising from or in connection with this DPA.

Annexes

- Annex A – Description of processing and contact information
- Annex B – Technical and organisational measures

Annex A – Description of processing and contact information

Additional Business Purposes and specific instructions regarding the processing

Nature of the processing

☒ collection
☐ recording
☒ organization
☒ structuring
☒ storage
☒ adaptation or alteration
☒ retrieval
☒ consultation
☒ use
☒ disclosure by transmission, dissemination or otherwise making available
☐ alignment or combination
☒ restriction, erasure or destruction of data (whether or not by automated means)
☐ other (please specify): _____

Categories of Data Subjects

☐ Processor employees and/or consultants
☐ Customers of Controller
☒ Users of the following service/website/application: MyTurtleAdmin, the FlatTurtle meeting room booking platform, and the Wi-Fi and building networks managed or monitored by FlatTurtle
☐ Other (please specify): _____

Categories of Personal Data

☒ Personal identification data (*name, address, telephone number, etc.*)
☒ Electronic identification data (*IP address, MAC address, cookies, etc.*)
☐ Financial data (*bank account numbers, insurance, salary, etc.*)
☐ Personal characteristic (*age, gender, date of birth, place of birth, citizenship, visas, etc.*)
☐ Psychological data (*opinions about personality, etc.*)
☐ Family (*marital status, cohabitation, name of spouse/partner, children, parents, etc.*)
☐ Memberships (*professional and non-professional memberships, clubs, groups, associations, etc.*)
☐ Judicial data (*data concerning convictions and offences, suspicions, indictments and administrative sanctions*)
☐ Housing characteristics (*address, type of home, residence time, etc.*)
☐ Health related data (*physical health, mental health, genetic data, treatments, prescriptions, etc.*)
☐ Education (*curriculum, financing of studies, qualifications, professional experience, publications, etc.*)
☐ Profession and job (*current job, work description, job application data, career, salary, data concerning IT equipment, passwords and codes, etc.*)
☐ Pictures or videos
☐ Other (please specify): _____

Retention period

☒ During the Term

☐ Specific retention periods, please specify: _____

Contact information for the person responsible for data protection compliance

Processor	
Full name	FlatTurtle legal contact
Title	Data protection contact
E-mail	legal@flatturtle.com
Phone number	+32 2 669 10 01

List of Sub-Processors

Company name	Contact information for the person responsible for data protection compliance	Location of processing	Nature of sub-processing (description of services)
GitLab	about.gitlab.com/privacy/	US	Code hosting
Google	support.google.com/a/answer/2888485?hl=en	US	Email and document storage
GCP, Google APIs	support.google.com/maps/answer/10400210?hl=en	US	APIs & web services
Mailchimp	mailchimp.com/legal/data-processing-addendum	US	Mail communication - newsletters
Mailgun	www.mailgun.com/gdpr	EU	Sending of automated emails from the FlatTurtle applications
Leaseweb	www.leaseweb.com/en/about-us/legal/personal-data-protection-acts	EU	Server hosting
Moneybird	www.moneybird.nl/privacy	NL	Invoicing
NextDNS	nextdns.io/privacy	EU	DNS services
Cloudflare	www.cloudflare.com/cloudflare-customer-dpa/	Global, incl. US	Hosting of the FlatTurtle applications, their databases and file storage; DNS, network security and content delivery
Better Stack	betterstack.com/dpa	EU	Log management and monitoring
Ubiquiti	www.ui.com/legal/privacypolicy/	US	Cloud management of Wi-Fi networks (UniFi)
Anthropic	www.anthropic.com/legal/privacy	US	AI assistance in support and operation of the FlatTurtle applications
Teltonika (RMS)	www.teltonika-iot-group.com/policies-certificates/privacy-policy	EU	Remote management of 4G routers

Annex B – Technical and organisational measures

Physical access controls

The FlatTurtle servers are located in secure server facilities that comply to strict access standards

System access controls

Only necessary personnel have access to the systems which are protected with the standard system protections.

Data access controls

Access to databases or other means of storing personal information is heavily restricted.

Data backups

Regular backups are taken and off-site backups stay within the EU.