Data Processing Agreement (DPA)

This document (“referred to as **“DPA”** or **“Contract”**) is an annex to the Software as a Service Agreement (SaaS) (hereinafter referred to as the **"Main Agreement**") between Spacewise Ltd., Rotfluhstrasse 63, 8702 Zollikon, Switzerland (hereinafter referred to as the **"Processor**") and the Customer according to the Main Agreement.

1. Subject of the Contract

1.1. In addition to the Main Agreement, this Contract regulates the processing of the Customer's personal data by the Processor. The purpose of the data processing and the list of the groups of persons and types of data concerned are contained in Annex 1 to this Contract.

1.2. The provisions of the Swiss Data Protection Act (DSG) and, insofar as the processing falls within the scope of the European General Data Protection Regulation (GDPR), the provisions of the GDPR shall apply to this Contract.

1.3. The Contract regulates in particular the data protection measures within the meaning of art. 10a FADP and art. 28 GDPR and the rights and obligations of the Customer and of the Processor to fulfill the requirements of the FADP and the GDPR.

2. Rights of the Customer

2.1. The Customer is responsible for the data processing within the scope of this Contract. When collecting, processing and using his data, he is responsible for checking the permissibility and compliance with the applicable data protection provisions as well as for safeguarding the rights of the data subjects.

2.2. The Processor may only collect, process and use the Data within the scope of this Contract and as instructed by the Customer. Use for other purposes, including the Processor's own purposes, is not permitted, except the tenant of the Customer has explicitly agreed.

2.3. The Customer reserves the right to issue instructions on the type, scope and procedure of data processing within the framework of the Main Agreement.

2.4. Changes to the types of data processed and procedural changes shall be mutually agreed and documented.

2.5. Instructions may be issued by the Customer in general or in individual cases. They must be given in writing. Individual instructions may also be given verbally, but must be confirmed in writing by the Customer without delay. The Customer shall name to the Processor those persons who are authorized to issue instructions.

3. Obligations of the Processor

3.1. The Processor shall act exclusively within the framework of the agreements made and in accordance with the Customer's instructions.

3.2. The Processor assures that it complies with the requirements of Art. 10a DSG and Art. 28 GDPR and verifies and documents the fulfillment of its legal obligations through regular internal controls.

3.3. Data processing only takes place on the territory of Switzerland and in the European Economic Area (EEA). Data processing in other countries (so-called third countries) is only permissible with the prior written consent of the Customer and if the relevant legal requirements are met.

3.4. The Processor undertakes to support on-site inspections of the Customer by prior arrangement, to provide the necessary documents and information and to provide all necessary information within a reasonable period of time in the event of data protection and data protection-related inspections by the supervisory authorities.

3.5. The Processor shall assist the Customer in fulfilling the obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to the Processor.

3.6. If an instruction of the Customer violates the applicable data protection provisions, the Customer shall be notified thereof by the Processor.

3.7. The Processor undertakes to inform the Customer immediately of any breaches of the data protection provisions.

3.8. If the Customer's data at the Processor are endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties or if they have to be disclosed to third parties, in particular authorities, the Processor shall notify the Customer thereof without undue delay. The Processor shall immediately inform all persons responsible in this context that the Customer has dominion over the data.

3.9. Services pursuant to Sections 3.4 and 3.5 shall be provided against compensation at the hourly rates pursuant to the Main Agreement.

4. Technical and organisational measures for data security

4.1. The Processor is obliged to observe the principles of proper data processing and to monitor compliance with them.

4.2. Processor shall ensure the installation and maintenance of the necessary and appropriate data protection measures in accordance with Art. 7 DPA and Art. 32 GDPR. The binding technical and organisational measures are listed in Annex 2 and form part of this Contract.

5. Rights of the data subjects

5.1. If a data subject asserts claims under data protection law (e.g. the right to information), the Processor shall support the Customer in fulfilling the claims.

5.2. If a data subject contacts the Processor directly to assert his/her rights (in particular Art. 8 DPA and Chapter 3 GDPR), the Processor shall forward the request to the Customer without delay.

6. Subcontractors

6.1. The Processor may subcontract data processing; currently these are the subcontractors as per Appendix 1 to this DPA. The Processor shall inform the Customer prior to any intended change. The Customer may reject a subcontractor without giving reasons, whereby a rejection by the Processor shall entitle the Customer to terminate the Contract without notice.

6.2. The Processor shall carefully select the subcontractor and only engage third parties that meet a security standard appropriate to the performance of the task. The contractual agreements with the subcontractor shall be designed in such a way that they comply with the data protection provisions of this Contract, in particular by providing sufficient guarantees that appropriate technical and organizational measures are taken to ensure that the processing is carried out in accordance with the legal provisions.

6.3. The subcontracting relationship shall be concluded in writing in accordance with Art. 28 GDPR, whereby the Customer shall also be granted a right of inspection and control. The Customer shall bear any costs for this. Processor shall provide a copy of the subcontract and all necessary information upon request.

6.4. Not to be understood as a subcontracting relationship in the sense of this regulation are such services which are used by order Processors of third parties to support the execution of the order, e.g. telecommunication services or maintenance.

7. Control rights of the Customer

7.1. The Processor shall provide the Customer with all necessary information to demonstrate compliance with the obligations set out in this Contract.

7.2. The Customer is entitled to request written information and evidence of the data protection measures taken and their technical and organizational implementation.

7.3. The Customer may satisfy itself of the adequacy of the measures taken to comply with the technical and organizational data protection requirements at the Processor's premises before the start of the Data Processing and then at regular intervals after prior coordination. The Processor shall enable such verifications, provide the necessary information and offer the necessary support

7.4. The audits shall be conducted without avoidable disruption to Processor's business. Unless otherwise specified for urgent reasons to be documented by the Customer, the checks shall take place after reasonable advance notice and during the business hours of the Processor and not more frequently than every 12 months. If the Processor demonstrates that the agreed data protection obligations have been implemented correctly, the checks should be limited to spot checks.

7.5. Services of the Processor pursuant to this Section 7 shall be compensated at the hourly rates pursuant to the Main Contract.

8. Confidentiality

8.1. The parties undertake to treat all documents and data made available to them in connection with the execution of the order as well as the work results as confidential and, in particular, not to make them available to unauthorized persons.

8.2. Persons involved in data processing are prohibited from processing personal data without authorisation. This prohibition shall remain in force even after the termination of the activity. The persons concerned shall be bound in writing to data secrecy.

8.3. These obligations shall also apply after termination of the Contract.

9. Duration and termination of the Contract

9.1. The term of this DPA shall be governed by the Main Agreement.

9.2. The Customer acknowledges that it may extract the Data from the Processor's platform as a CSV file at any time. Upon termination of this Contract, the Processor shall securely delete or destroy all data carriers and all data (including any copies or duplicates made) upon request as instructed by the Processor, unless there is a legal obligation to store the Personal Data.

9.3. This obligation applies to the same extent to any subcontractors.

10. Final provisions

10.1. In all other respects, the final provisions pursuant to the Main Agreement shall also apply to this DPA.

Annex 1 - Information on the processing of personal and other data

1. Nature and purpose of the processing

The processing is carried out by storing the data on the systems of the Processor, enabling access by employees of the parties or transmission to the Customer via the Internet, transmission to third parties on behalf of the Customer, deletion of the data. The processing serves the fulfillment of the Main Agreement (Software as a Service).

2. Categories of persons concerned

The categories of data subjects concerned by the processing are the following: (1) Tenant of the Customer and (2) Employees/freelancers of the Customer.

3. Type of data processed

The following data are processed (personal and other data):

a) Tenant of the Customer

Master data	e.g. first name, last name, date of birth, letter salutation, address, customer number, location, e-mail, correspondence language, mobile phone, telephone, tenant, tenant organization, note, status, customer group, damage reports
Transaction	e.g. number, rental object, start of rental, end of rental, total price, payment
Payment	e.g. date, description, payment, CC number, reference no.
Usage data	e.g. rental object, rental start, rental end, status, settlement status, price total, payment
Rental property booked	e.g. name, picture, location category sub-category object group active from, active to, brand, model, inventory number, serial number, seasonal scheme, deposit
Accessories booked	e.g. accessory name brand, model, quantity, price, total price
Service booked	e.g. Name, For accessories, No. of objects, Percentage, Fixed price, For accessories. Objects, percentage, fixed price, No. of time units Time unit, price, time-based price, final price, currency, no. of bids, percent, price. Offers, Percent, Price
Surcharges / Discounts	e.g. description, amount

b) Employees/freelancers of the Customer

Master data	e.g. first name, last name, date of birth, contact, email, correspondence language, mobile phone, phone, fax, office location, username, account, email

4. Subcontractor

The Contractor may engage the following subcontractors:

a. Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA;
b. Datatrans Ltd., Kreuzbühlstrasse 26, 8008 Zürich, Switzerland;
c. Customer.io (Peaberry Software, Inc.), 9450 SW Gemini Dr, Ste 43920, Beaverton, Oregon, 97008, USA;
d. Segment.io, Inc., 100 California Street, 7th Floor, San Francisco, CA 94111, USA;
e. Stripe, Inc., 354 Oyster Point Blvd, South San Francisco, California 94080, USA;
f. RunMyAccounts AG, Grundstrasse 16b, CH-8712 Stäfa, Switzerland;
g. Close.com, PO Box 7775 #69574 San Francisco, CA 94120-777, USA;
h. Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855, Luxembourg;
i. Sendgrid, 1801 California St. Denver, Colorado 80202, USA;

Appendix 2: Organizational and Technical Measures of Data Security

1. Confidentiality

1.1. Access control: Protection against unauthorized access to data processing systems, e.g. keys, smart cards, electric door openers, porters, alarm systems, video systems.

1.2. Access control: Protection against unauthorized system use, e.g. passwords (including corresponding policy), automatic locking mechanisms, two-factor authentication for administrators, encryption of data.

1.3. Access control: No unauthorized reading, copying, modification or removal within the system, e.g. standard authorisation profiles on a "need to know"-basis, standard process for authorisation allocation, logging of accesses, periodic review of allocated authorisations, especially of administrative user accounts.

1.4. Classification scheme for data: Customer data is generally classified as confidential.

2. Integrity

2.1. Transfer control: No unauthorized reading, copying, modification or removal during electronic transmission or transport, e.g.: Encryption on data carriers and during transmission, Virtual Private Networks (VPN).

2.2. Input control: Determining whether and by whom personal data have been entered into data processing systems, changed or removed, e.g.: Logging.

3. Availability and resilience

3.1. Availability control: Protection against accidental or deliberate destruction or loss (also physical), e.g. backup strategy (online/offline; on-site/off-site): Backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS, diesel generator), virus protection, firewall, reporting channels and emergency plans; security checks at infrastructure and application level, multi-level backup concept with encrypted outsourcing of backups to an alternative data centre, standard processes in the event of staff changes/leavings.

3.2. Rapid recoverability.

3.3. Deletion periods: The following deletion periods apply to both the data itself, after deactivation of the account, and metadata such as log files, etc.: quarterly.

4. Procedures for regular review, assessment and evaluation

4.1. Data protection management, including regular employee training and Contractual obligation of employees.

4.2. Incident response management.

4.3. Contract control: No commissioned processing within the meaning of Art 28 GDPR without corresponding instructions from the Customer, e.g.: clear Contract design, formalized Contract management, strict selection of the Processor.

12 April 2022