Privacy Policy for StaySettle

Effective Date: 14 October 2025

Last Updated: 14 October 2025

1. Introduction

Welcome to StaySettle. This Privacy Policy explains how **SQVentures BV** ("we," "us," or "our") collects, uses, shares, and protects information in relation to our chargeback management services (the "Service").

This policy is designed to help you, our Customer ("you" or "Customer"), understand our data practices and to help you meet your own data protection obligations. By creating an account or using the Service, you acknowledge the practices described in this Privacy Policy.

2. Our Role: Data Processor

For the purposes of the EU General Data Protection Regulation (GDPR), it is essential to understand our respective roles:

- **You (the Hotel) are the Data Controller.** You own and control the personal data of your guests ("Guest Data"). You are responsible for the lawful basis of processing this data.
- **We (SQVentures BV) are the Data Processor.** We process Guest Data on your behalf and according to your instructions for the sole purpose of providing the Service as outlined in our Terms and Conditions.

This Privacy Policy primarily covers the data we collect directly from you (our Customer) and our role and responsibilities when processing Guest Data on your behalf.

3. Information We Collect

We collect information in two ways: information you provide directly to us, and information we process on your behalf from the services you connect.

3.1. Information You Provide to Us (Customer Data)

- **Account Information:** When you sign up, you provide your hotel name, your name, your role, and your email address. We also store your securely hashed password.
- **Business Information:** During onboarding, we may ask for your business name as it appears on guest statements and your hotel's phone number.
- **Third-Party Credentials:** To use the Service, you provide us with authorization tokens to connect to your Stripe account and, optionally, your Property Management System (PMS) account (e.g., Mews Client and Access Tokens). We securely store these tokens.
- **Uploaded Documents:** You may upload files to be used as dispute evidence, such as your cancellation policy.

3.2. Information We Process on Your Behalf (Guest Data)

Upon your authorization, our Service automatically accesses and processes the following data from your connected accounts:

- **From Stripe:** We process data related to disputed transactions, including charge details (amount, date, currency), card details (last four digits, country of origin), AVS/CVV check results, and billing details associated with the charge (cardholder name, email address, billing address).
- **From your PMS (e.g., Mews):** We process reservation data required to build an evidence case. This may include guest names, contact details, reservation status (e.g., Checked-in, Checked-out), booking source, confirmation numbers, stay dates, and details of incidental charges (folios).

4. How We Use Information

We use the information we collect and process for the following purposes:

- **To Provide and Maintain the Service:** To monitor for disputes, match disputes to reservations, gather and assemble evidence, and submit evidence packages to Stripe on your behalf.
- **To Manage Your Account:** To create and manage your account, provide customer support, and communicate with you about service updates or security alerts.
- **To Process Payments:** To calculate and automatically collect our commission fee for won disputes via Stripe Transfer, as authorized in our Terms and Conditions.
- **To Improve the Service:** We may use aggregated and anonymized data to analyze usage patterns and improve the functionality and accuracy of our Service. We will never use identifiable Guest Data for this purpose.

5. How We Share Information (Our Sub-processors)

We do not sell your data or your guests' data. We only share information with a limited number of third-party service providers (sub-processors) who act on our behalf to help us provide the Service. These include:

- **Cloud Hosting (Render):** Our application infrastructure is hosted on Render.
- **Database and Cloud Services (Google Cloud):** We use Google Cloud's Firestore to securely store your data and Guest Data.
- **Artificial Intelligence Services (Google Cloud):** We use Google Vertex AI to process and extract information from documents you upload. The content of your uploaded documents is shared with this service for analysis.
- **Payment Processing (Stripe):** We share evidence data back to Stripe to respond to disputes on your behalf. We also use Stripe to process our commission fees.

We have entered into data processing agreements with each of these sub-processors to ensure they uphold the same level of data protection and security that we do.

6. Data Security

We take the security of your data seriously and implement appropriate technical and organizational measures to protect it from unauthorized access, alteration, disclosure, or destruction. These measures include:

- Using secure, reputable cloud infrastructure.
- Encrypting data in transit and at rest.
- Hashing all user passwords using strong algorithms (Bcrypt).
- Restricting internal access to data to only those employees who require it to perform their job functions.

7. Data Retention

We retain your Customer Data for as long as your account is active. We retain Guest Data processed on your behalf for the duration required to manage the associated dispute and for a reasonable period thereafter to comply with legal obligations and auditing requirements. Upon termination of your account, we will delete your data in accordance with the procedures outlined in our Terms and Conditions.

8. Your Data Protection Rights (under GDPR)

As our Customer, you have certain rights regarding your personal data:

- **Right to Access, Rectify, or Erase:** You can review and update your account information through the Service's settings. You may also request the deletion of your account and associated data.
- **Right to Object and Restrict Processing:** You have the right to object to or request the restriction of our processing of your personal data under certain conditions.

Regarding Guest Data: As the Data Controller, you are responsible for responding to data rights requests from your guests. If a guest wishes to exercise their rights (e.g., access, erasure) regarding data that we process on your behalf, they must contact you directly. We will provide you with reasonable assistance to help you respond to these requests.

9. International Data Transfers

Our sub-processors (such as Google Cloud and Render) may be based in the United States or other countries outside the European Economic Area (EEA). When we transfer data to these sub-processors, we rely on legally-provided mechanisms to lawfully transfer data across borders, such as the EU-U.S. Data Privacy Framework or Standard Contractual Clauses (SCCs).

10. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. We will notify you of any material changes by posting the new policy on this page and, where appropriate, through other means such as email. We encourage you to review this policy periodically.

11. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact our Data Protection Officer at:

SQVentures BV

Attn: Data Protection Officer

Quellijnstraat 19a, Amsterdam

KvK-nummer: 98488961

Email: qzeegers@sqventuresbv.com